IRONSCALES

IRONSCALES Fall 2024 Threat Report

Deepfakes: Assessing Organizational Readiness in the Face of This Emerging Cyber Threat

Deepfake-driven security concerns are quickly spreading and rapidly intensifying, with over three quarters of IT professionals expressing serious concerns about what the near future holds.

Executive Summary

As cybersecurity threats continue to evolve, organizations are facing a growing and increasingly sophisticated security challenge: deepfakes. Once considered a fringe technology, deepfakes have quickly emerged as a threat to corporate security, with their ability to seamlessly mimic voices, faces, and identities. This rise in deepfake-driven attacks, particularly through email—an already vulnerable communication channel—has put IT and security professionals on high alert.
To better understand the depth of this concern, IRONSCALES conducted a survey of over 200 cybersecurity professionals spanning a wide range of roles, industries, and specializations to explore their views on deepfakes and the evolving landscape of email security. The findings reveal a very real security concern: while email remains a critical tool for business operations, it's also the primary channel for the next wave of cyberattacks, combining the old threat of phishing with the new weapon of deepfakes.

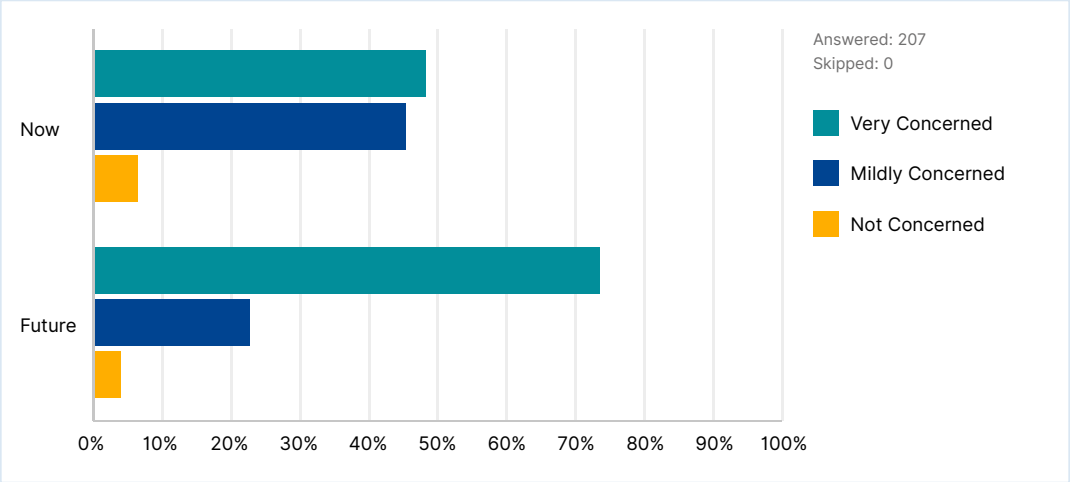
A look into the survey data shows an overwhelming 90% of respondents believe that deepfake phishing threats are evolving either "very quickly" or "moderately," pointing to a significant challenge for organizations to stay ahead of these increasingly sophisticated attacks, especially as traditional phishing methods become enhanced by deepfake technology. As a result, 64% of those surveyed expect deepfake-enabled cyberattacks to increase over the next 12-18 months, surpassing other forms of attacks such as ransomware and account takeover. The data suggests that deepfakes are quickly rising to the top of the cybersecurity concern list and organizations may not be fully prepared to combat them yet. These statistics underscore the urgency for organizations to adapt their defenses against deepfakes, especially as these threats are evolving and expected to grow in frequency.

Key Findings

1 Concerns around deepfakes are increasingly widespread and rapidly intensifying

- Over 94% of IT professionals express some level of concern about the threat deepfakes currently pose to their organizations.
- Nearly half (48%) say they are “very concerned” with the threat currently posed by deepfakes.
- When asked about the threat deepfakes will pose in the near future, the percentage of “very concerned” respondents rose sharply, to a staggering 74%.

Q2 When considering deepfake threats in general (image, video, voice, email), how would you rate your concern about the risks to your organization both now and in the future?



	Very Concerned	Mildly Concerned	Not Concerned	Total	Weighted Average
Now	48.31% 100	45.41% 94	6.28% 13	207	1.58
Future	73.66% 151	22.44% 46	3.90% 8	205	1.30

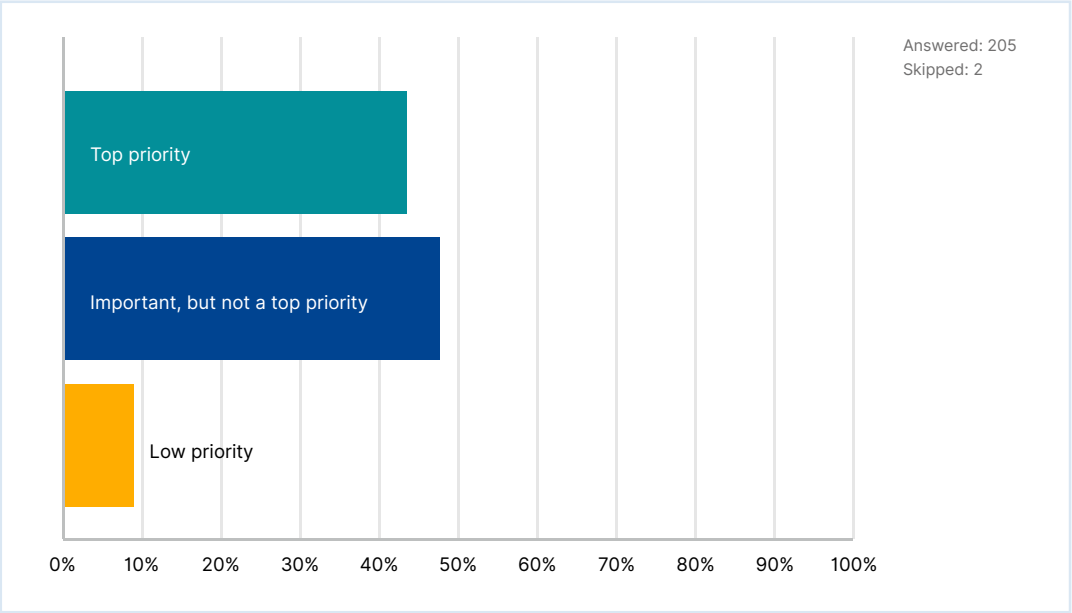
While concerns about the risks deepfakes pose to organizational security are already near-universal, it’s clear that IT professionals see them primarily as an emerging threat—one whose true potential for harm has not yet been realized. When asked to rate their overall level of concern regarding deepfakes both now and in the future, the percentage of respondents saying they were “very concerned” with the immediate risk they pose was just below one half (48%). However, when considering the organizational risks deepfakes will pose in the near future, the share of respondents expressing serious concern rose sharply, to a staggering 74%.

Over
94%
of IT professionals
express some level of concern about the threat deepfakes currently pose to their organizations.

2 Deepfake defense is quickly climbing toward the top of organizations' priorities

- Over 43% of IT professionals say deepfake defense will rank as their organizations' top security priority in the next 12-18 months.
- An additional 48% acknowledge that it will be an important part of their security operations.

Q12 In the next 12-18 months, how does deepfake defense rank among your organization's security priorities?



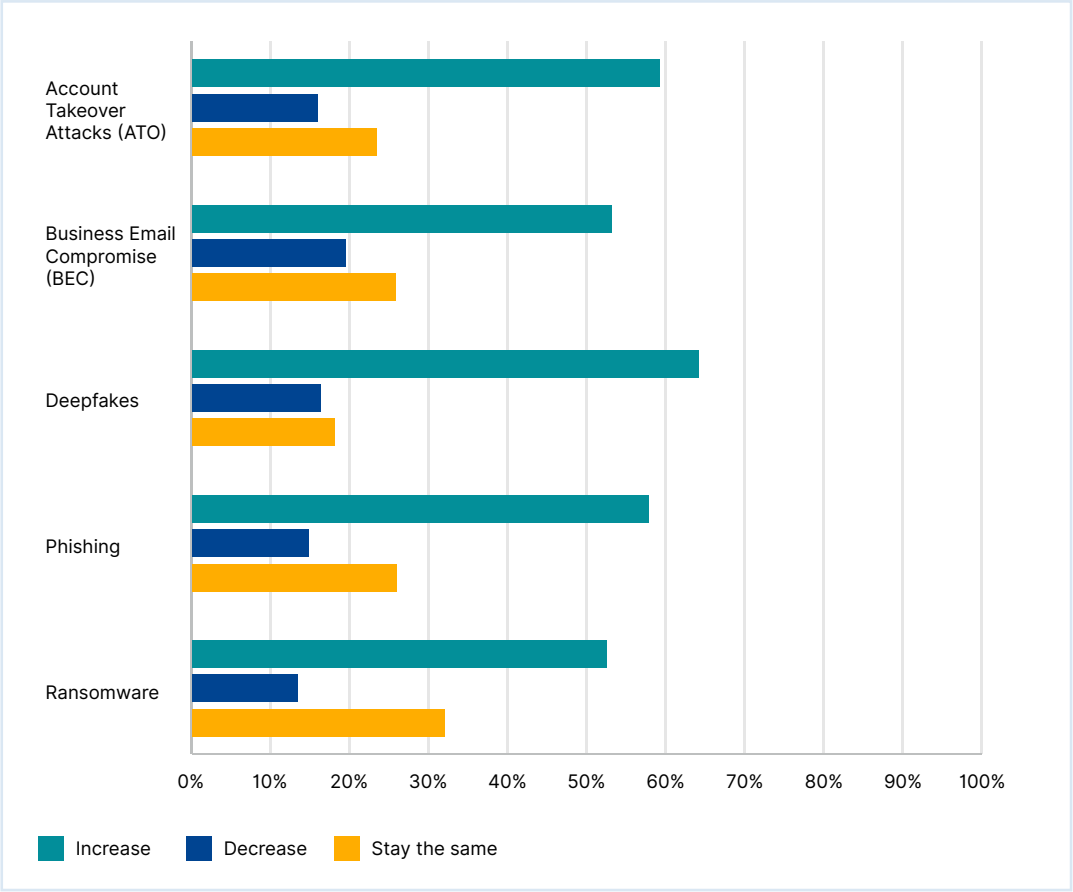
Over 43% of IT professionals say deepfake defense will rank as their organizations' top security priority in the next 12-18 months.

While most IT professionals seem to view deepfakes primarily as an emerging threat, they show little doubt as to the gravity of that threat once fully realized. With over 90% of respondents anticipating deepfake defense to be an important part of their security operations within the next year and a half, it's clear that this technology's potential for organizational and societal harm is looming large on the minds of many in the industry.

3 Most IT professionals agree—deepfake-enabled attacks are set for serious growth, surpassing other forms of attacks such as ransomware and account takeovers

- 64% of respondents say they expect the volume of deepfake-enabled attacks to increase over the next 12-18 months, which is more than any other attack type listed, including ransomware, phishing, account takeover (ATO) and business email compromise (BEC).

Q7 Over the next 12-18 months, do you expect the following threats against organizations (not yours specifically) to increase, decrease, or stay the same?



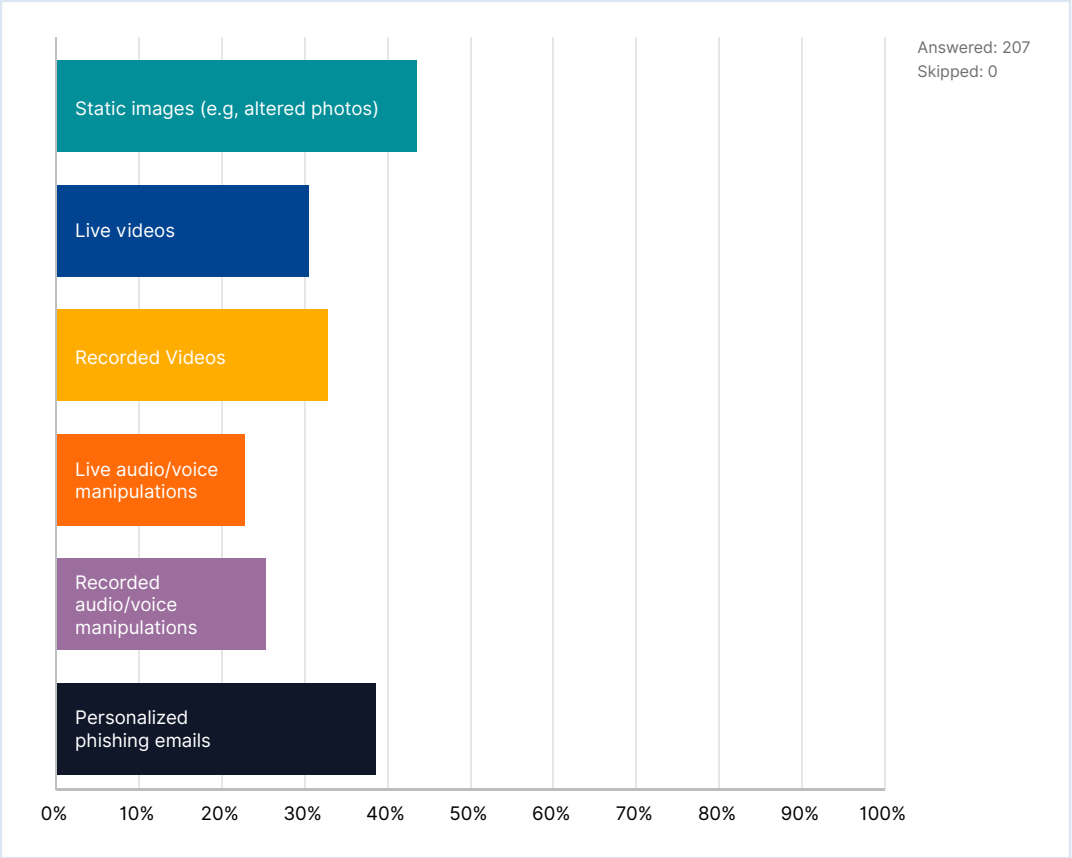
64%
of respondents say they expect the volume of deepfake-enabled attacks to increase over the next 12-18 months.

In addition to rapidly ascending the industry's list of priorities, the survey also suggests that we'll see a similar rise in the volume of deepfake-enabled attacks against organizations. The annual number of all cyberattacks has been increasing steadily for some time. However, our cohort showed the strongest agreement in expected growth when it came to deepfakes. The two nearest competitors, account takeover (ATO) and phishing, saw 59% and 58% of respondents say they are likely to increase, respectively.

4 Email emerges as the most commonly-used and worrying avenue of attack for deepfake-driven threats

- Targeted phishing emails are the second most commonly-encountered type of deepfake-driven cyber attacks today, surpassed only by static imagery, and by a margin of just 5%.
- The majority of professionals (53%) believe email represents an "extreme threat" as a channel for deepfake-driven attacks, surpassing all other avenues, including social media and messaging apps.

Q4 Which types of deepfakes has your organization encountered in the past year (select all that apply)?



75%
of respondents reported that their organizations had experienced at least one deepfake-related incident within the last 12 months.

In the present survey, 75% of respondents reported that their organizations had experienced at least one deepfake-related incident within the last 12 months. Of those who had, 39% said one or more of those incidents had come in the form of personalized phishing emails — making it second only to static imagery as the most commonly-encountered form of deepfake attacks. Later, when asked how much of a threat various channels posed as avenues for deepfake-driven attacks, "Email" emerged as the most worrying medium — with 53% of respondents characterizing it as "an extreme threat," and an additional 39% rating it as a "moderate threat."

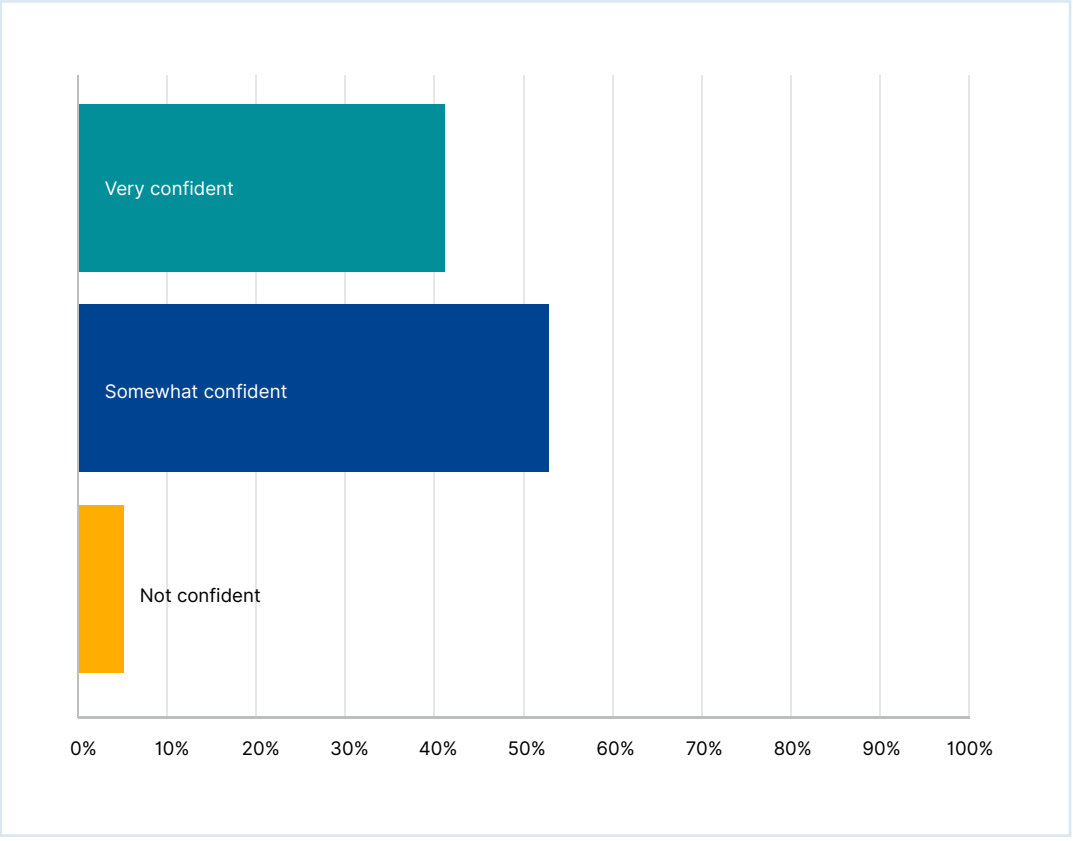
5 Despite current deepfake initiatives and future investments in protection, organizations are still not particularly confident in their ability to defend against deepfakes.

- 68% of respondents reported that their organizations have already begun providing specialized cybersecurity training related to the identification of deepfakes.
- Nearly three quarters (73%) of respondents say their organizations will invest in deepfake protection within the next 12 months.
- However, a startling 60% of respondents are only 'somewhat confident' or 'not confident' in their organization's ability to defend against deepfake threats.

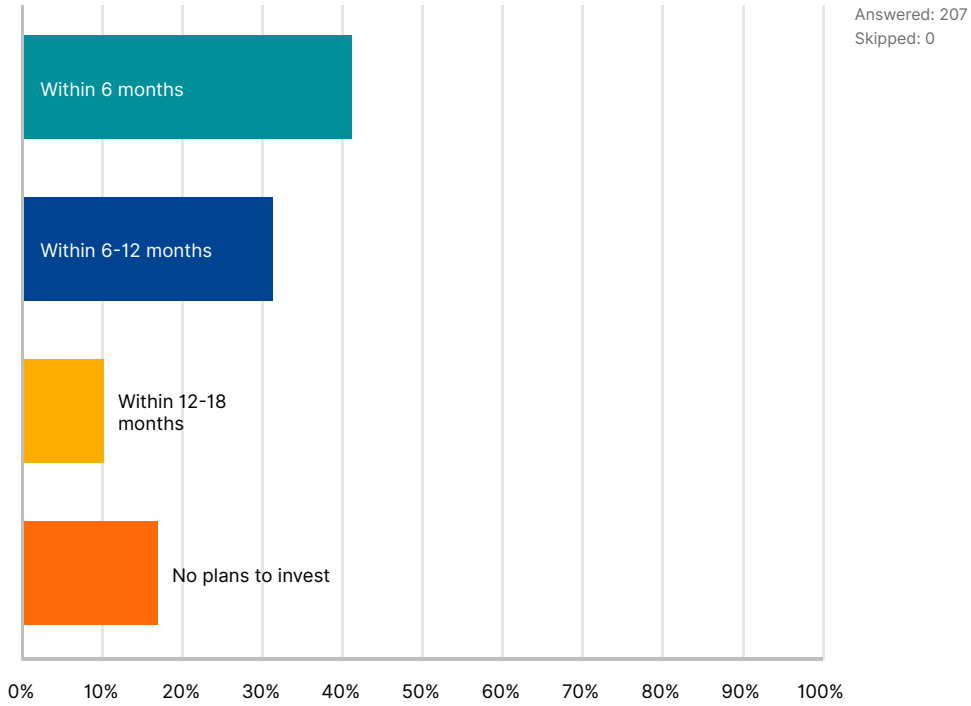
A startling 60% of respondents are only 'somewhat confident' or 'not confident' in their organization's ability to defend against deepfake threats.

Nearly three quarters 73% of respondents say their organizations will invest in deepfake protection within the next 12 months.

Q8 How confident are you in your organization's ability to defend against deepfake threats?



Q14 When does your organization plan to invest in deepfake protection?



Answer Choices	Responses	
Within 6 months	41.55%	86
Within 6-12 months	31.40%	65
Within 12-18 months	10.14%	21
No plans to invest	16.91%	35
Total		**207**

68%
of respondents reported that their organizations have already begun providing specialized cybersecurity training related to the identification of deepfakes.

Again, although most professionals seem to agree that deepfakes' true security implications have yet to take shape, it appears most expect matters to worsen rapidly. With so many organizations already having instituted training programs, and an overwhelming majority planning to invest in deepfake-specific security measures within the next 12 months, it's hard to imagine that these organizations are simply "getting well ahead" of the problem.

One interesting point to note is that, despite the unmistakable air of concern around deepfakes today and the fact that over 67% of respondents have already begun providing cybersecurity training related to identifying deepfakes, only 41% of respondents are very confident in their organizations' ability to defend against deepfake threats, which is cause for concern.

Conclusion & Recommendations

With tight budgets and a whole lot of unknowns still on the horizon, organizations will undoubtedly look to be selective in their approach to defending against deepfake-driven threats. By identifying the most worrying channels, such as email and messaging platforms, organizations will be able to prioritize effectively in the short term. However, as is true of nearly all emerging threats, it likely won't be long before threat actors begin to pivot — developing and diversifying their tactics in response to defensive efforts from the industry.

While predicting the nature of tomorrow's threat landscape is always fraught with uncertainty, the overwhelming consensus that deepfakes present a serious and rapidly worsening security threat is impossible to ignore. Proactive organizations would be wise to invest in defensive technologies, dedicated awareness training, and even simulation testing to ready their workforce for what increasingly appears to be an inevitable wave of deepfake-driven threats.

Methodology

IRONSCALES conducted a survey of 207 IT & cybersecurity professionals, via a popular digital polling platform, spanning a wide range of roles, industries, and specializations to explore their views on deepfakes and how this emerging threat impacts organizational security. The data was collected and analyzed in August/September 2024.

About IRONSCALES

IRONSCALES is the leader in AI-powered email security protecting over 15,000 global organizations from advanced phishing threats. As the pioneer of adaptive AI, we detect and remediate attacks like business email compromise (BEC), account takeovers (ATO), and zero-days that other solutions miss. By combining the power of AI and continuous human insights, we safeguard inboxes, unburden IT teams, and turn employees into a vital part of cyber defense across enterprises and managed service providers. IRONSCALES is headquartered in Atlanta, Georgia.

To learn more about advanced phishing protection, visit **www.ironscales.com** or schedule a demo with IRONSCALES: **ironscales.com/demo**