LUMEO

ABNORMAL AI

SURVEY FOR K-12 EDUCATION PROFESSIONALS: EMAIL SECURITY CHALLENGES

INTRODUCTION

Lumeo partnered with Abnormal AI to better understand how K12 organizations are combating email security threats. We heard from K12 professionals to learn which challenges are most prominent, how concerned they are about protections, and future priorities to mitigate email security risks.

We surveyed over 50 professionals within the K12 industry across roles and in primarily Executive and Director level roles. Titles included; Chief Academic Officer, Chief Financial Officer, Chief Operations Officer and Chief Human Resources Officer.

KEY OBSERVATIONS

K12 Organizations continue to face growing email security threats, with phishing, malware, social engineering, and vendor email compromise ranking as top concerns. While many organizations are satisfied with their current solutions, gaps in automation and management efficiency remain. IT teams dedicate significant time to mitigating email threats, yet challenges such as limited staffing and delayed reporting hinder swift response. AI-driven security is gaining traction, though some organizations remain uncertain about its effectiveness.

Compliance requirements, including FERPA, HIPAA, and state privacy laws, shape email security strategies for many organizations. Despite these regulations, confidence in handling emerging threats varies, with service disruptions and data breaches remaining key consequences. Budget constraints and deployment complexity continue to slow adoption of advanced security measures. As email-based attacks grow more sophisticated, K12 organizations are prioritizing AI and automation to strengthen their defenses.

98% respondents say their organization has encountered **phishing attacks** in the past year, making it the most common email security threat.

36% respondents say their IT teams spend over **6 hours per week** managing email security incidents, but staffing limitations and delayed reporting remain major challenges.

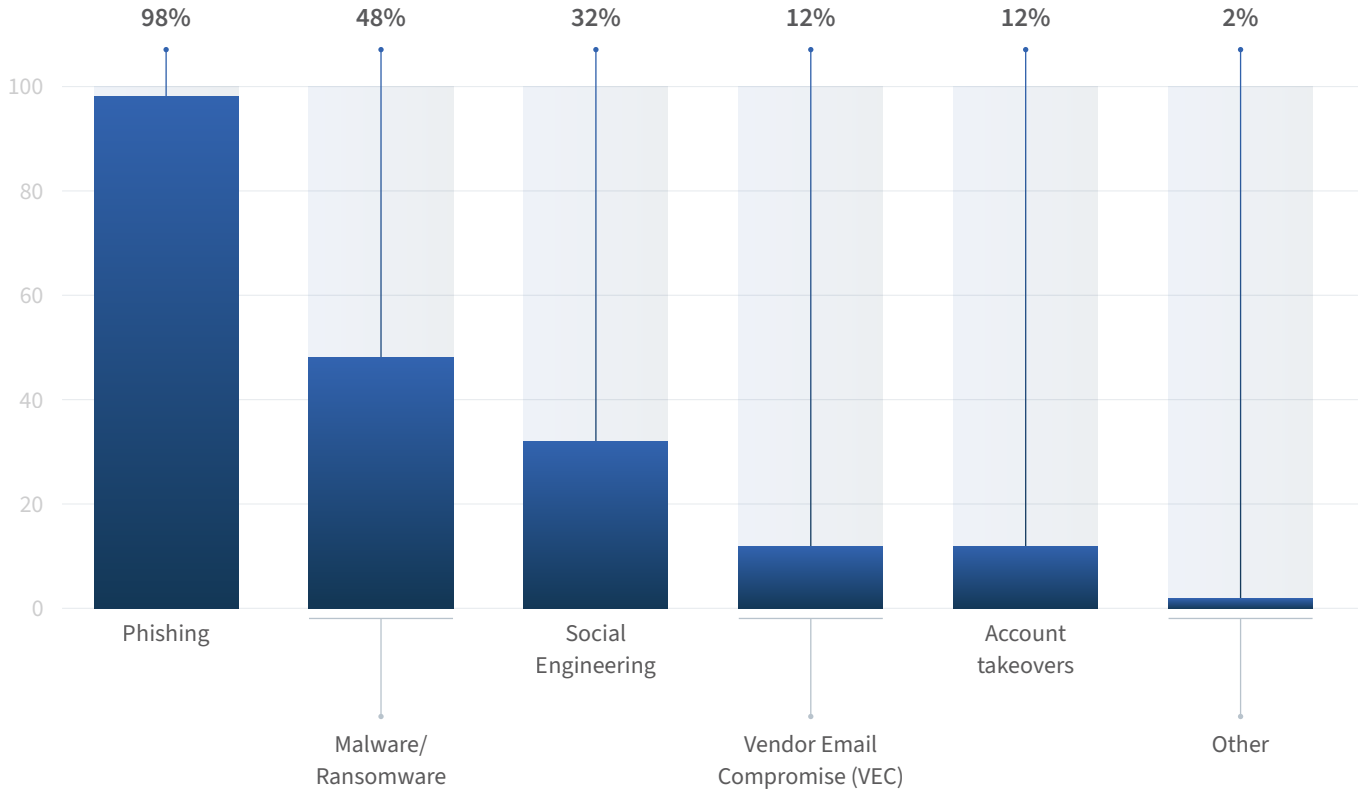
40% respondents say **compliance requirements** such as FERPA, HIPAA, and state privacy laws drive their email security strategies.

72% respondents cite **budget constraints** as the biggest barriers to adopting advanced email security solutions.

SURVEY TRENDS

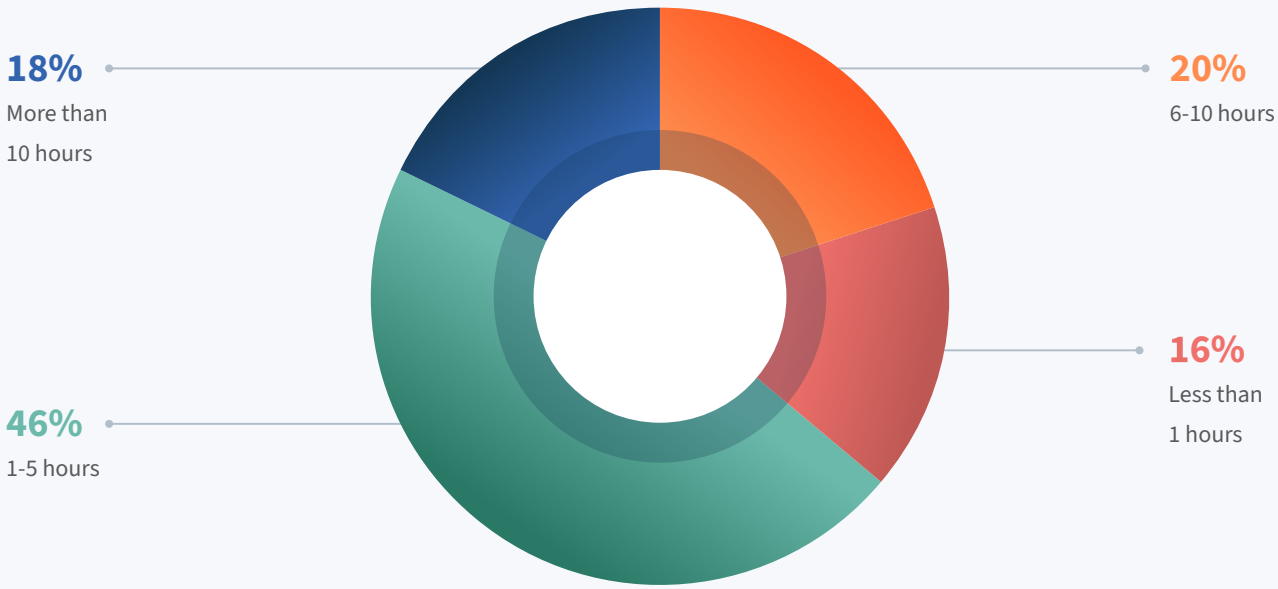
Phishing dominates, while malware, social engineering, and vendor attacks persist.

What types of email threats has your organization encountered in the past year?



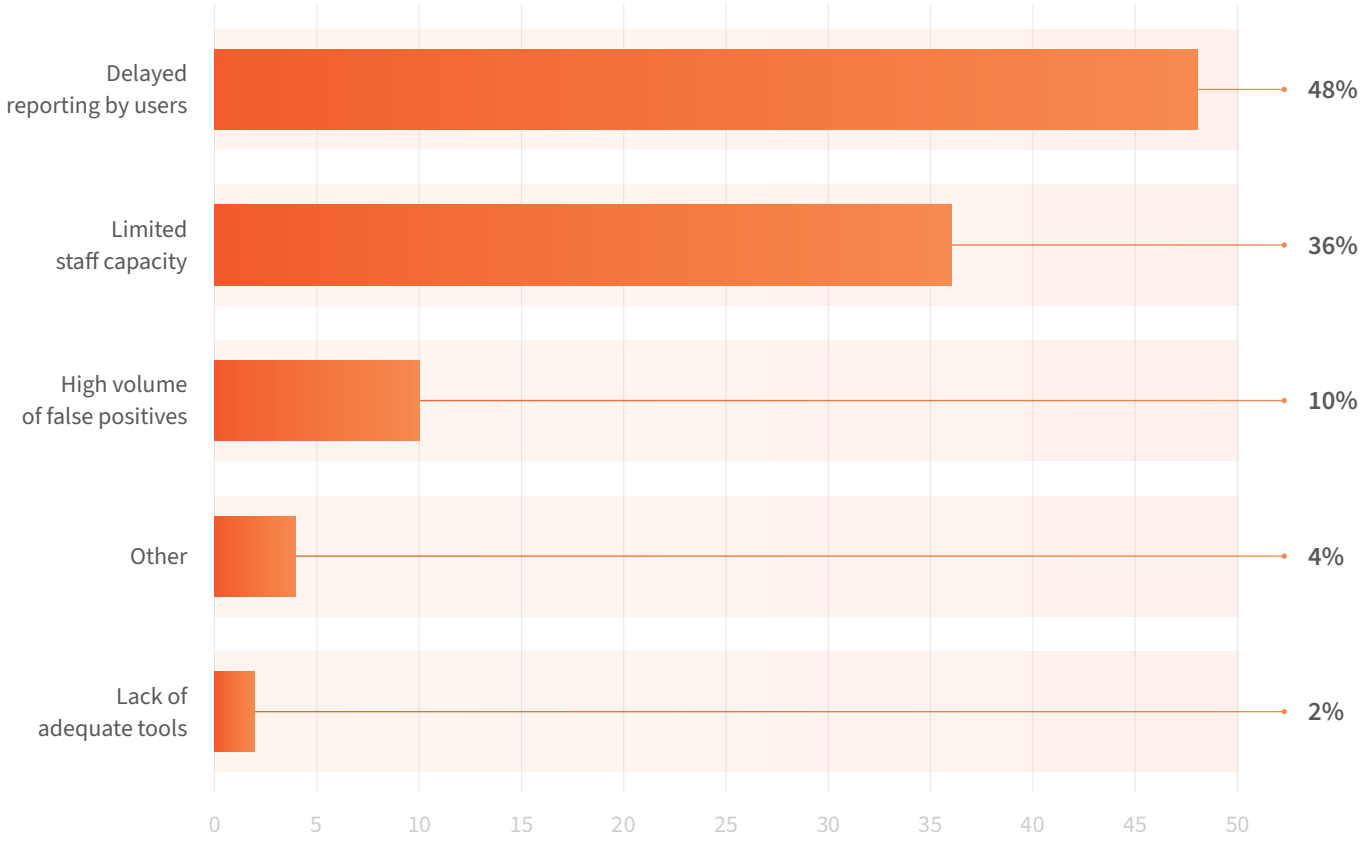
Nearly half of IT teams spend 1-5 hours weekly on email security, but some face heavy burdens.

On average, how much time per week does your IT team spend managing email security incidents?



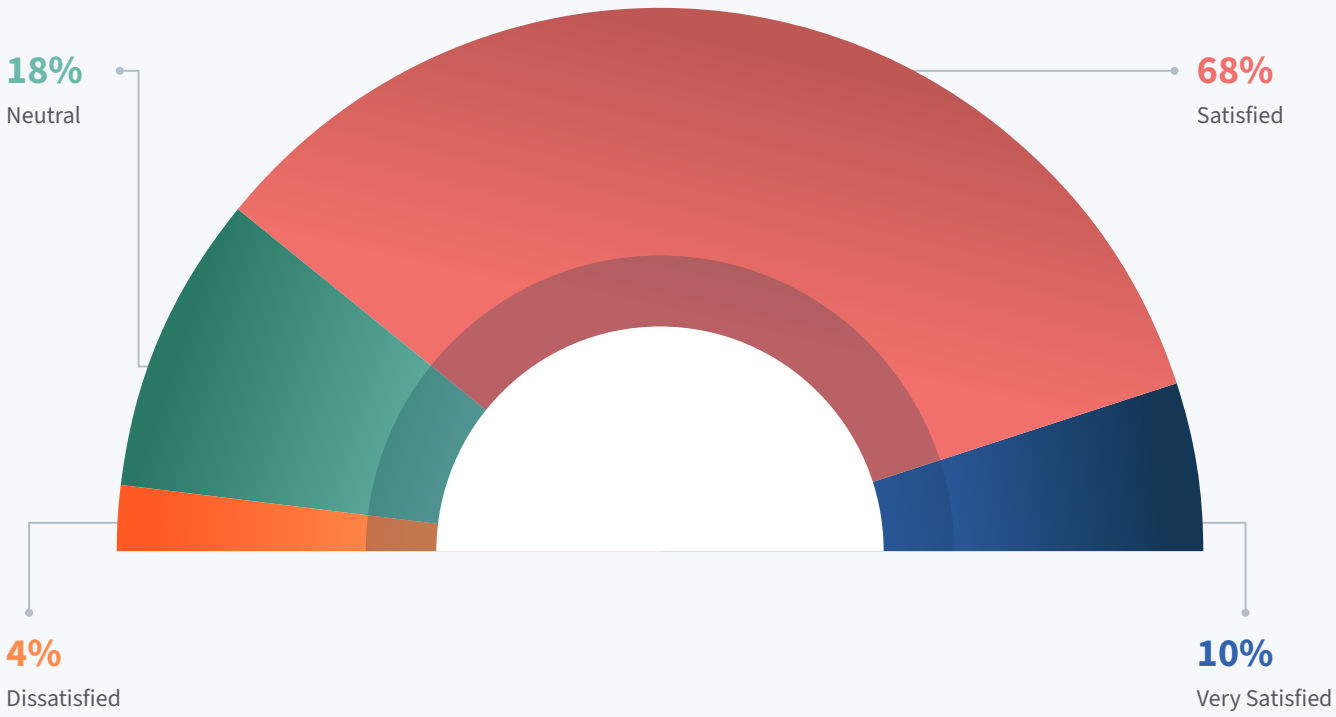
Delayed reporting and limited staff are the biggest barriers to phishing response.

What is the biggest challenge your team faces when handling user-reported phishing attempts?



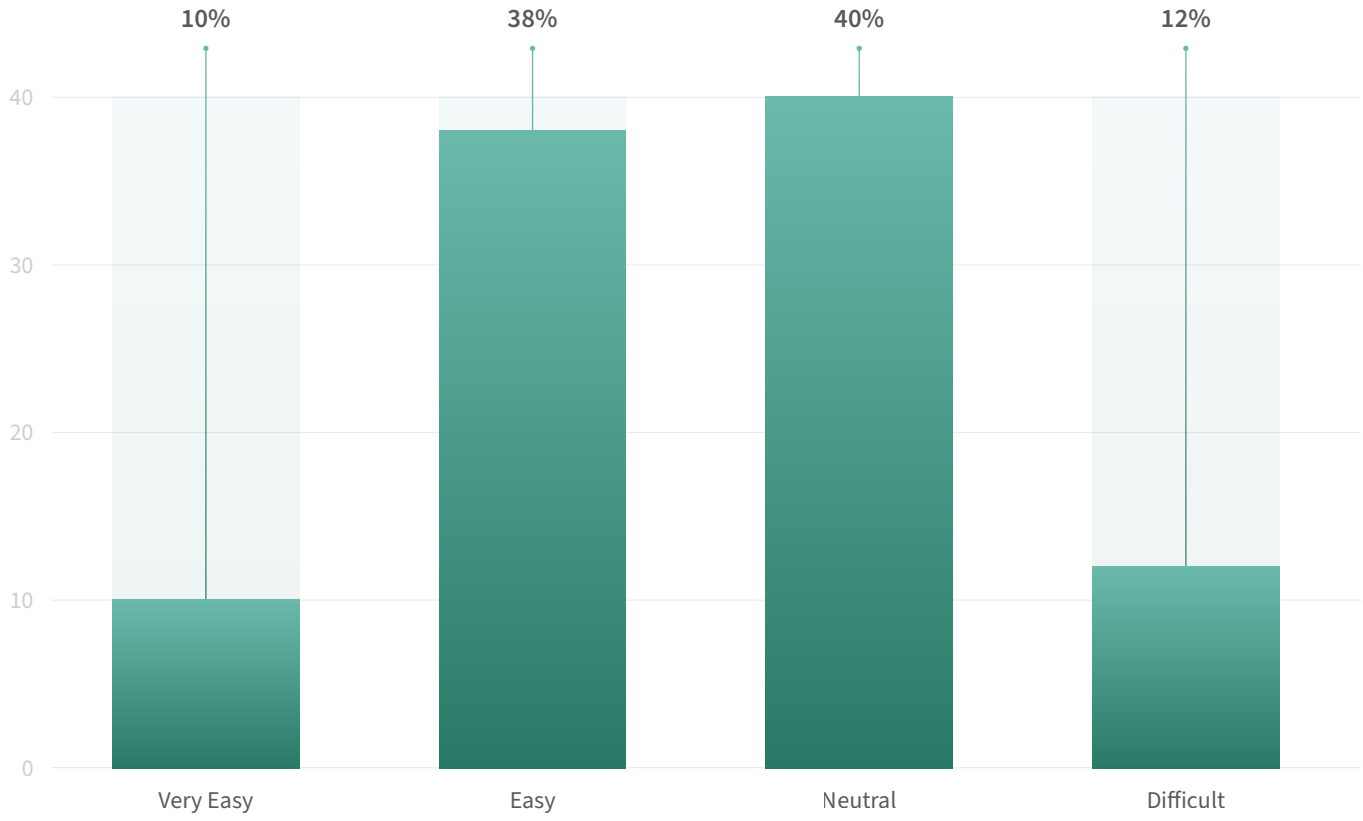
Most organizations are satisfied with email security, but gaps remain.

How satisfied are you with your current email security solutions?



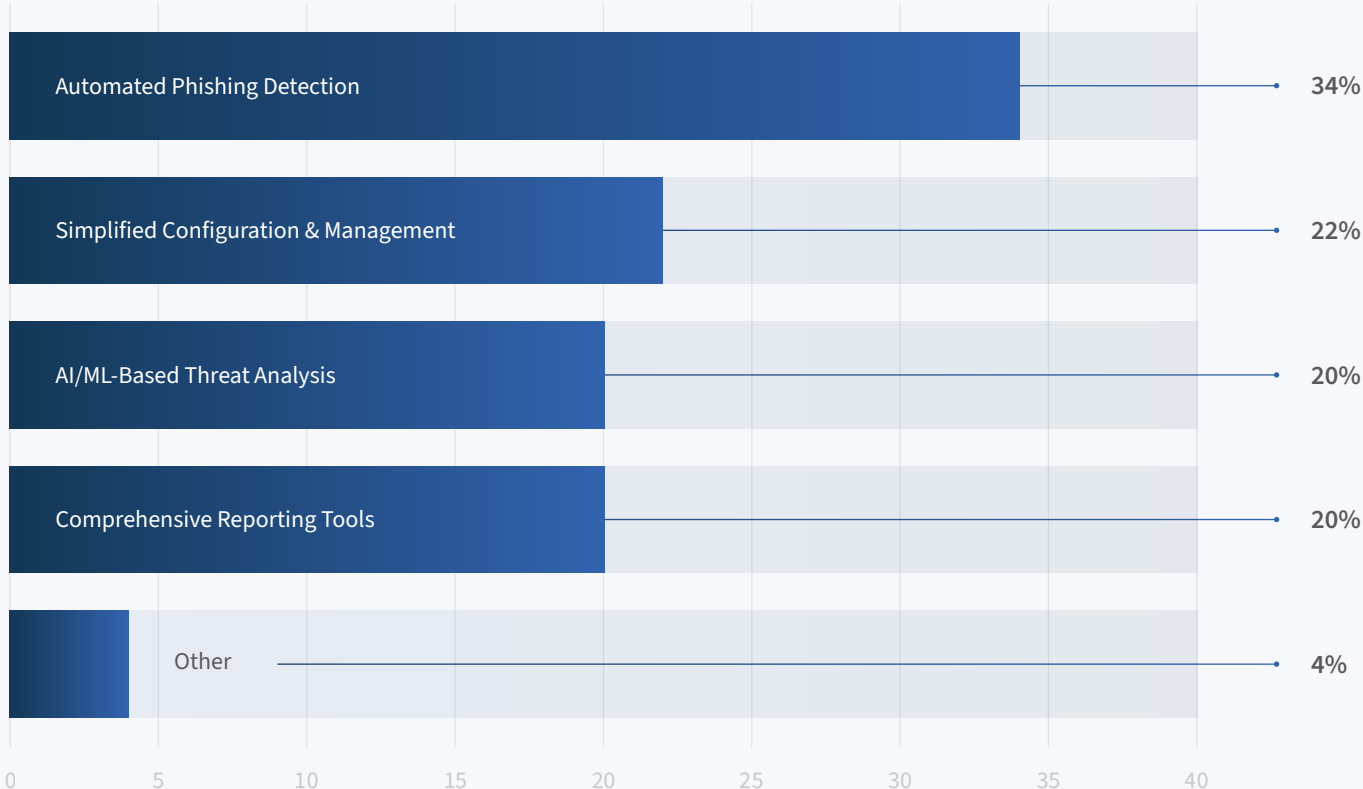
Email security management is manageable for most, but not effortless.

How would you rate the ease of configuring and managing your current email security tools?



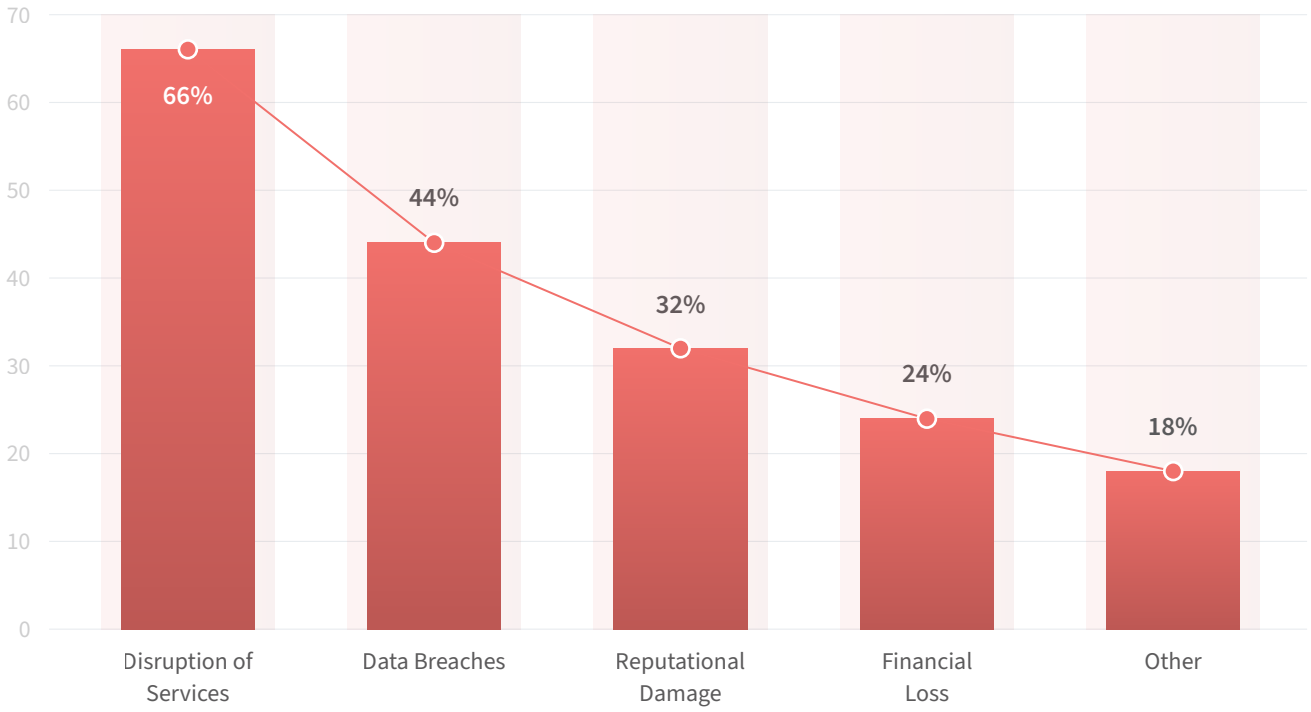
Automation, AI, and better management are the top missing features in email security.

What is the most significant feature you feel is missing from your current email security solution?



Service disruptions and data breaches are the leading consequences of email threats.

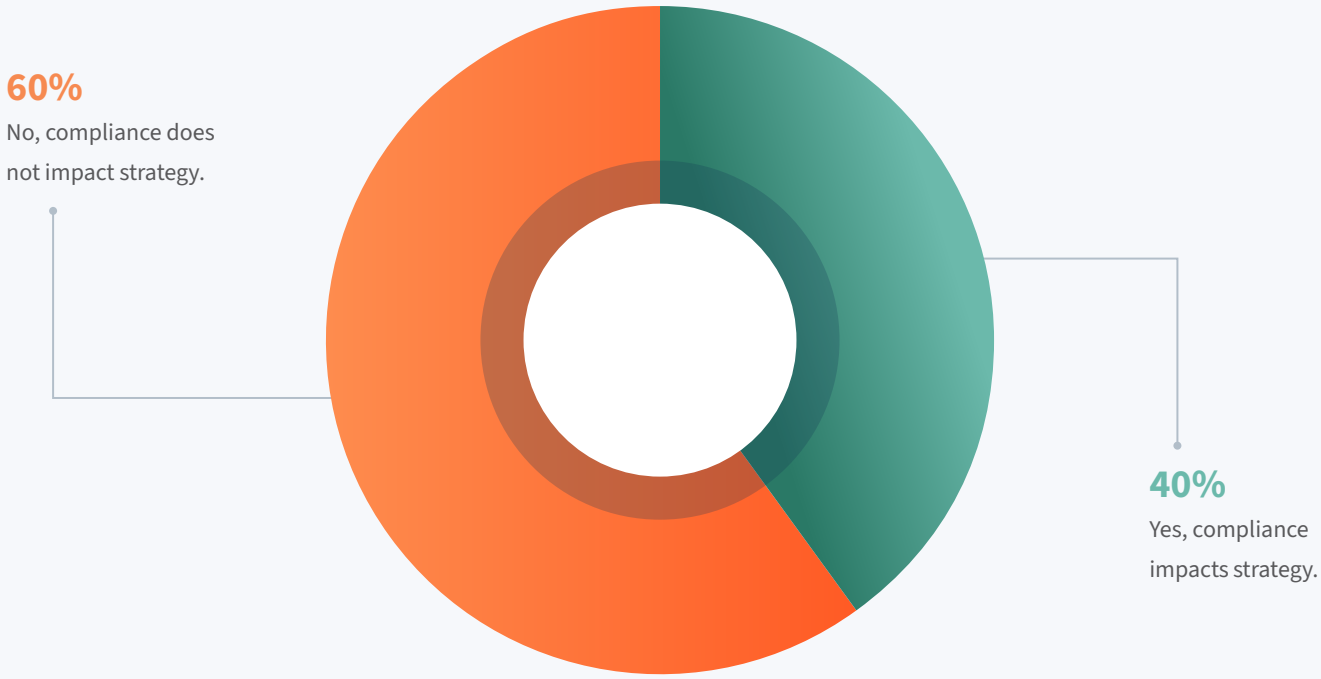
What financial or operational impacts has your institution experienced due to email-based threats?



Other: None, Capacity, This is not my department

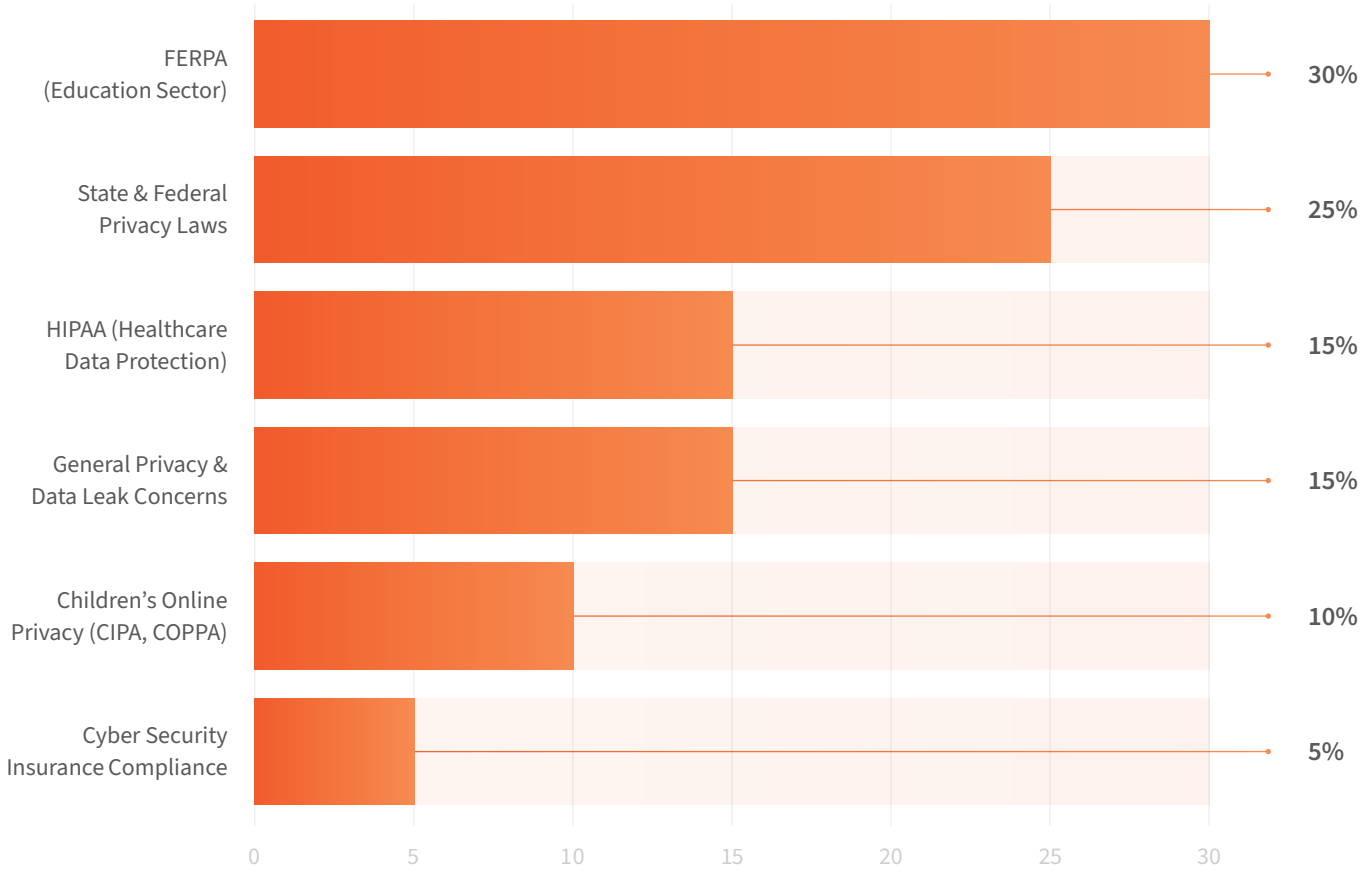
Compliance drives email security for 40% of organizations.

Does your institution face compliance requirements that impact your email security strategy?



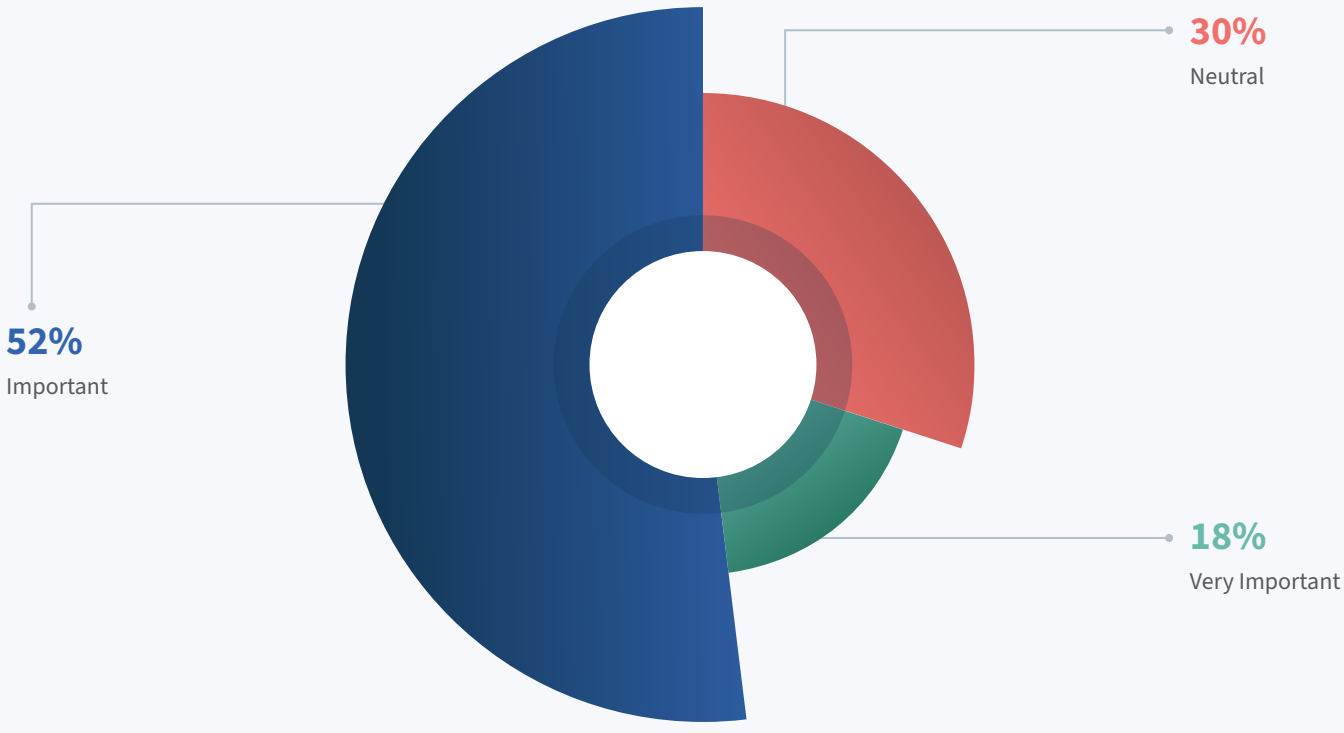
FERPA, HIPAA, and state privacy laws are key drivers of email security compliance.

Please specify which compliance requirements impact your email security strategy.



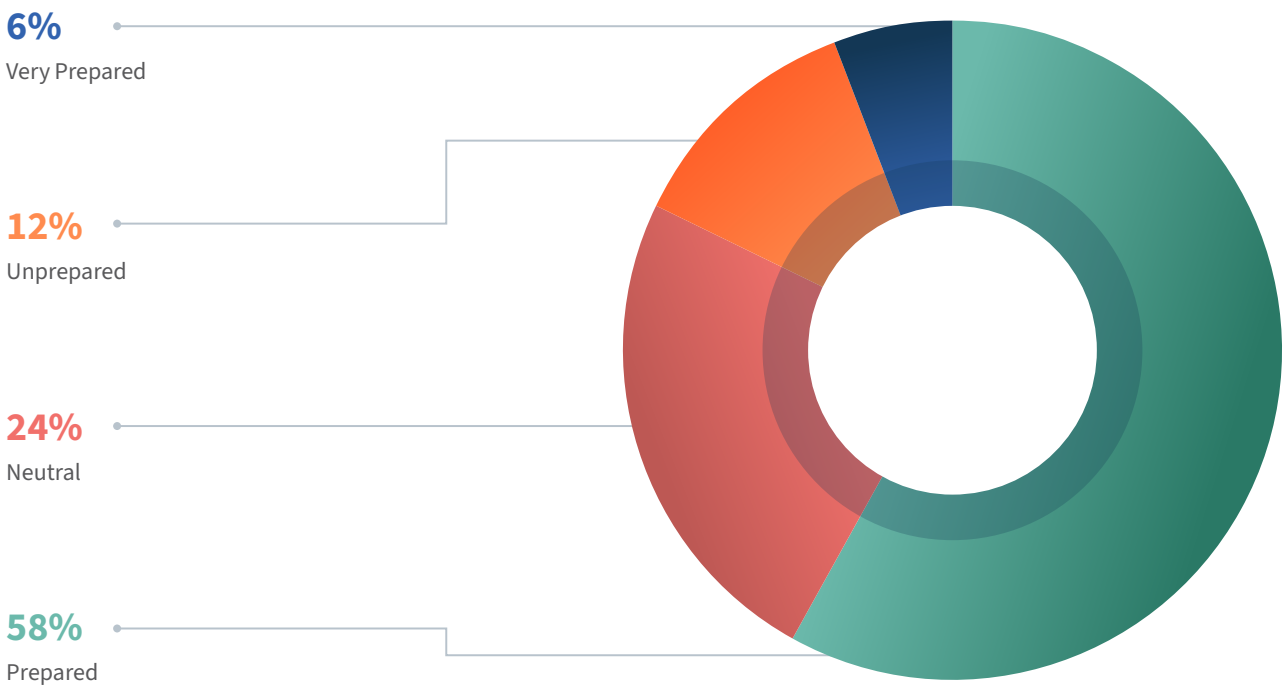
AI-powered email security is a priority for most, but some remain neutral.

How important do you consider AI/ML-driven solutions in addressing email-based threats?



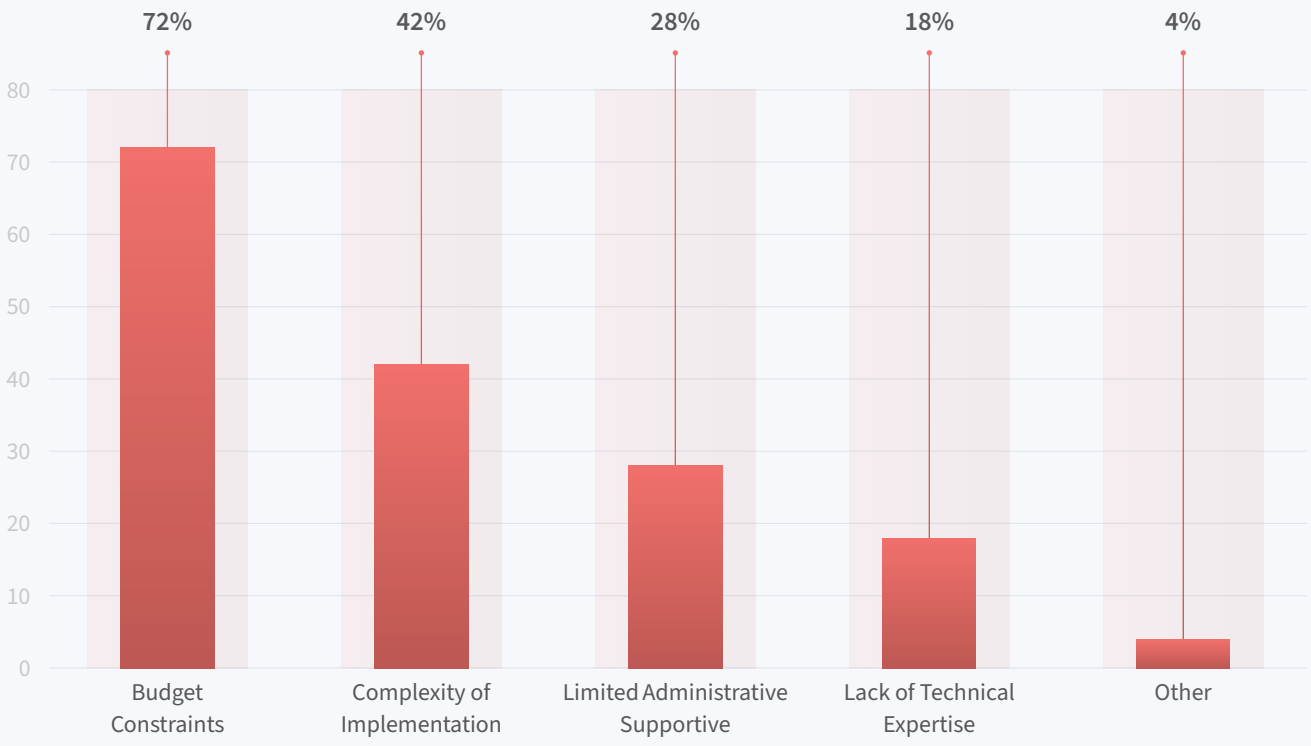
Most organizations feel prepared for novel email threats, but confidence levels vary.

How prepared do you feel your institution is for handling novel email-borne attacks?



Budget and complexity are the biggest barriers to advanced email security adoption.

What are the primary barriers to adopting advanced email security solutions?



Other: This isn't my department; We have an advanced email security solution

Is there anything else you would like to share about email security challenges in your institution? (optional)

Other challenges:

The state is causing a problem with their lack of security

Budget constraints are the primary barrier to adopting advanced email security solutions.

It is an ongoing challenge

About Abnormal AI

Abnormal AI is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages contextual signals to analyze the risk of every cloud email event—detecting and blocking sophisticated, socially-engineered attacks that target human vulnerability.

Abnormal is designed to be deployed in minutes via an API integration with Microsoft 365 or Google Workspace, unlocking the full value of the platform instantly. Additional protection is available for Slack, Workday, ServiceNow, Zoom, and multiple other cloud applications. Abnormal is currently trusted by more than 3,200 organizations, including 25% of the Fortune 500, as it continues to redefine how cybersecurity works in the age of AI.

Learn more

Abnormal

LUMEO