

Collaboration Security.



risks and realities of the
modern work surface



Global survey reveals heightened complexity
of securing IT environments amid rapid
collaboration tool adoption

13:20 ✓✓

introduction. | ✓✓

The continued rise in the use of collaboration tools provides a new threat surface for cybercriminals to infiltrate.

As cyber threats multiply in sophistication and volume, they become concentrated in platforms that are irresistible to cybercriminals. These platforms, such as Microsoft 365, increase organizations' exposure and vulnerability to attacks. The reason is simple: The rise of online collaboration among employees and the consolidation of email and collaboration tools has created a tantalizing environment for cybercriminals that requires just one entry point to result in potentially devastating effects.

In the modern work surface, few organizations can function without the use of email and collaboration tools. Software suites and their add-ons, such as Microsoft Teams, Google Workspace, and Slack, integrate communications and messaging with project management functions. Designed to provide a central platform for data and document sharing, collaboration software encourages virtual teamwork and helps companies work more efficiently in the context of today's remote and hybrid work environments.

While email remains the primary route of attack for cybercriminals, the continued rise in the use of collaboration tools provides a new threat surface for cybercriminals to infiltrate. The Gartner™ Market Guide for Email Security states that "although email is still the most common attack vector, many attackers use emails to begin the communication and then move it to Slack, Teams or any other collaboration platforms." This creates even more risk for security leaders to manage, underscoring the need for more comprehensive security awareness training as well as holistic cybersecurity protections across all communications tools.

Facing an onslaught of attacks while the attack surface expands to include collaboration tools and hybrid work environments is the new norm for users and security teams. As a result, it has become business-critical for organizations to secure collaboration platforms as quickly as possible.

collaboration tools



a dangerous threat vector.

Mimecast commissioned a survey of 600 cybersecurity leaders and over 3,000 employees to gauge their understanding and conduct related to collaboration tool security within their organizations. The survey revealed that despite cybersecurity leaders' confidence in their cyber readiness (74%), the threat of attacks via collaboration tools remains immense, and almost all organizations have suffered a cybersecurity threat stemming from them.

The impacts of these breaches are substantial, including loss of company data, customers, reputation, and significant financial costs, no matter the company's size, region, or industry.

94% 

of organizations have experienced a threat via collaboration tools



Small companies are least confident in their cyber readiness compared to companies of other sizes. Only 66 percent feel their organization is very prepared or extremely prepared to deal with a cybersecurity breach via collaboration tools.

Ninety-four percent of the organizations surveyed have experienced a threat via collaboration tools. A damaged company reputation is a looming threat that cybersecurity leaders are concerned about with collaboration tool security compromise, given financial cost of these attacks on organizations can be steep. The average total cost of collaboration-tool-based attacks on any given organization in the past year was over \$574,783 – which includes costs like additional security measures, additional staff, and systems recovery.



Username



total cost of collaboration-tool-based attacks
on any given organization

\$574,783 av.

\$1 million

Sixteen percent of those surveyed estimate the total cost of attacks via collaboration tools in the past year at over \$1 million. This number climbs to 30 percent in the US and 18 percent in the U.K.

It stands to reason that the cost of a collaboration-tool-based attack is lower for smaller businesses than it is for larger companies – with a small organization averaging \$410,522 in losses. This is likely because SMBs are targeted less frequently by cybercriminals since they have less money to extract.

All organizations, however, can mitigate the costs of collaboration-tool-based attacks by implementing or shoring up existing security awareness training. Ensuring that users are continually and effectively trained on how to use collaboration tools with security in mind can help reduce the number of cyberattacks that find their way into an organization via collaboration tools, resulting in less time, resources, and money spent on remediation.

a gap in awareness training perception

Given the speed at which organizations began using collaboration platforms as a critical business tool, dedicated training for employees all but fell by the wayside. Yet security teams and cybersecurity leaders within these organizations believe they are providing sufficient collaboration tools training for employees.

cybersecurity
leaders vs.
employees.

85%



38%



A full 85 percent of cybersecurity leaders feel their organization has effectively communicated the security vulnerabilities of collaboration tools to their employees, but 38 percent of employees claim they have not received any collaboration tools security training.



leaders.

Cybersecurity leaders claim to carry out collaboration tool security training, with the vast majority believing they are effectively communicating risks and best practices to employees.

In fact, 100 percent claim their organization carries out some form of cybersecurity training for collaboration tools, with 70 percent claiming to do so monthly or quarterly.

100%

A full 85 percent say their organization has effectively communicated the risks and realities of collaboration tools to their employees.

85%



employees.

Yet, only a very small proportion of employees feel they have had specific awareness training to address collaboration tools.

In fact, 38 percent claim they have not received any collaboration tools security training, and only 10 percent say they have received dedicated collaboration tools security training separate from the wider cybersecurity training offered by their organization.

38%

Thirty-one percent have received collaboration tools security training as part of the wider cybersecurity training offered by their organization and 21 percent received this as part of their onboarding process.

31%

+10%

Smaller companies are less likely to train their employees than larger organizations, which presents a much bigger cybersecurity risk for these companies. Nearly half (48%) of employees at small companies said they have not received collaboration tool security training, a full 10% more than those at larger organizations.

These results demonstrate that employees have been trained much more extensively on email security than collaboration security, but security leaders cannot assume that employees are applying the same rigor when it comes to security in collaboration tools as they are with email.

As collaboration tool adoption grows even further, training on tools like Microsoft Teams or Slack must become a clear and equivalent part of security awareness training.

Indeed, employees are demonstrating riskier behaviors when using collaboration tools than when using email. As the thinking goes, it's easy for users to assume that every person using the same collaboration tool is a genuine member of their organizations since the tool appears to operate in a closed environment. But once a threat actor compromises a platform like Microsoft 365, they can easily impersonate others. The fact is, employees are less likely to screen documents sent via collaboration tools than sent via email. And with collaboration tools seeming more personal, employees are less likely to question requests they receive via collaboration tools as opposed to requests received via email.

To wit, nearly one-third (30%) of employees said they don't see themselves directly responsible for cybersecurity breaches on collaboration tools that involved their devices/accounts – compared with 18% of cybersecurity leaders.

Since most employees are not specifically trained on collaboration tool security, many said they would not feel personally responsible for a security breach.

 **employees ...**
30%

 **leaders ...**
18%

a greater danger: employee behavior



**collaboration tools
vs. email.**

Employees are surprisingly overconfident when it comes to using business collaboration tools. There is a significant gap between their understanding of collaboration tool security and specific behaviors when using collaboration tools. While most employees claim to understand the threat and alter their behaviors in different hybrid environments, many forget to make even the most basic security checks.



email ...

91%

state they conduct checks before clicking a link or opening an attached file



collaboration tools ...

79%

state they conduct checks before clicking a link or opening an attached file

Compared to email, employees let their guard down more when using collaboration tools – clicking links and opening attachments. Most employees (81%) claim to understand the security risks and best practices required of hybrid and remote work environments – and claim to alter their behavior accordingly (78%).

More specifically – and to further demonstrate their overconfidence – 61% of employees said they alter their behavior when working in a hybrid environment to stay more secure (e.g., check for encrypted connections when using a public Wi-Fi network), and 65% said that since the pandemic, they are more careful about what links they click when using collaboration tools.

In practice, these employees' behavior shows they are far more likely to let their guard down when using collaboration tools compared to when using email. They do perform fewer checks – the spelling of the source, the legitimacy of the attachment file name(s), and the URLs – before clicking on any links and/or attachments they have received via a collaboration tool compared to those they have received via email. For instance, 91 percent say they review spelling, links, or the email address of the sender within email applications like Microsoft 365, but within a tool like Microsoft Teams, that number drops to 79 percent.

Put differently, a full 1 in 5 employees skip all cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment.

Employees are at their most vulnerable when receiving a message from their line manager or via a team group chat/channel. Of those surveyed, 65 percent are likely to click on a link to an unfamiliar website or source if they receive it from their line managers, and 24 percent don't usually check anything before clicking on any links and/or attachments in a message on a team group chat/channel on a business collaboration tool.



1 in 5 employees skip all cybersecurity reviews before responding to a private message on a business collaboration tool with a link or an attachment.



65% are likely to click on a link to an unfamiliar website or source if they receive it from their line managers.

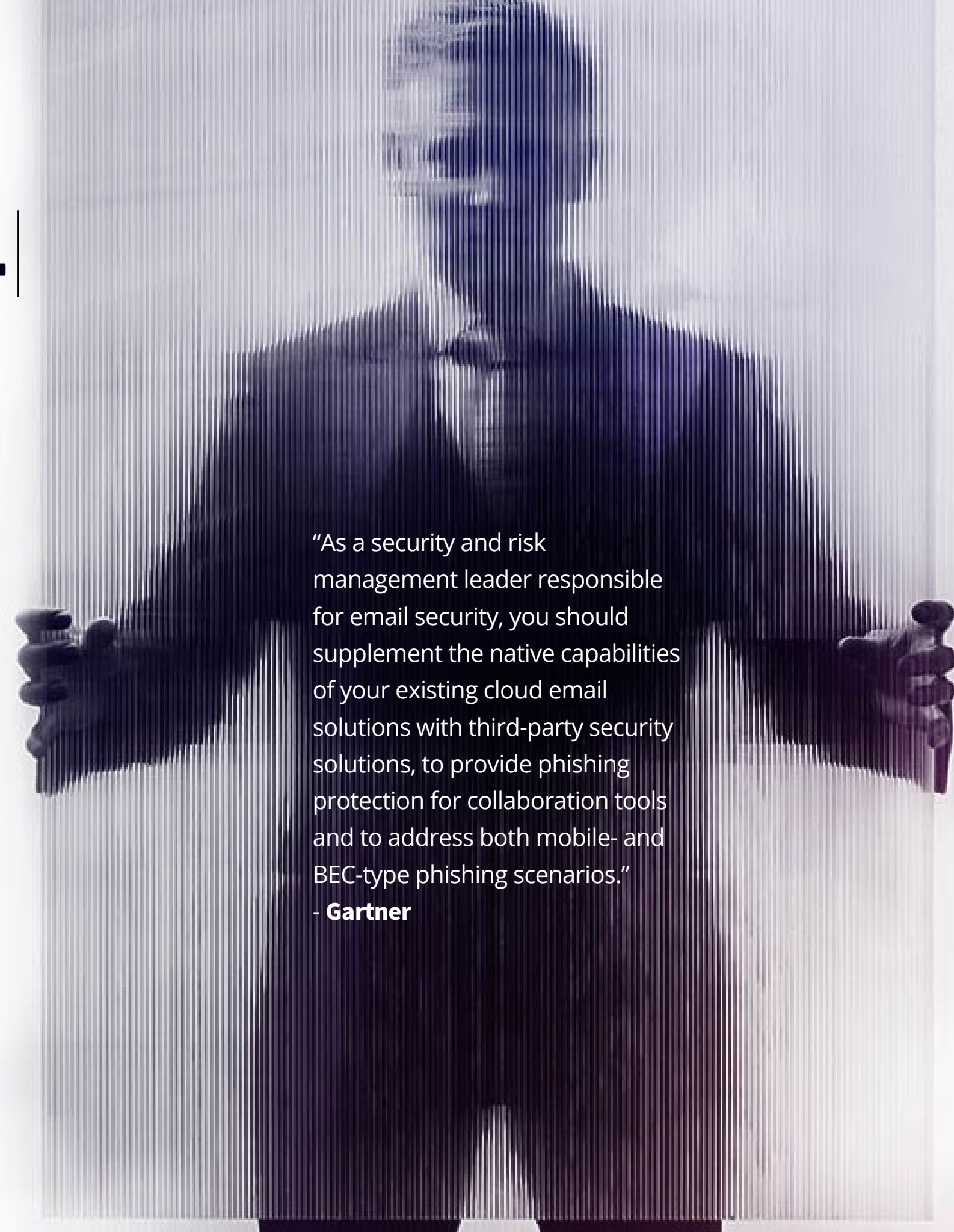


24% don't usually check anything before clicking on any links and/or attachments in a message on a team group chat/channel on a business collaboration tool.

key takeaways for cyber leaders.

Collaboration tools can be a fertile breeding ground for cybercrime. They pose a huge threat to organizations globally – and the impact of attacks extend well beyond financial costs.

The survey conducted by Mimecast revealed the heightened complexity of securing IT environments amid rapid collaboration tool adoption. Not only is this a technical challenge of securing the needed platform so that cybercriminals cannot gain entry, but it is also a cultural challenge of creating awareness and accountability throughout the organization.

A man in a dark suit and tie is speaking into a microphone. He is positioned on the right side of the frame, with his hands near the microphone. The background is a plain, light-colored wall.

“As a security and risk management leader responsible for email security, you should supplement the native capabilities of your existing cloud email solutions with third-party security solutions, to provide phishing protection for collaboration tools and to address both mobile- and BEC-type phishing scenarios.”

- **Gartner**

other key takeaways include:

Leaders must enforce training for collaboration tools.

Organizations should take the time to train employees on the specifics of not allowing messages that appear to come from their direct managers or any other leader within their companies to cause them to skip security review steps.

Organizations need holistic protections.

Bad URLs and attachments can do the same damage to businesses regardless of communications medium. Instead of disjointed security policies across email and collaboration tools like Teams, leaders must provide their organizations with holistic cybersecurity protections across the full environment.

Users must practice the same good security habits with collaboration tools as they do on email.

Employees do not fully understand the security implications of collaboration tools: they are not careful about what they share or click, despite claiming to understand the cyber risks and best practice when using them, and despite taking email security far more seriously.

Leaders overestimate their readiness.

Cybersecurity leaders are overestimating their organizations' readiness in combating cybercrime via collaboration tools, believing their employees are well-trained to deal with a breach of this kind, while employees do not feel they have had any dedicated training.

Employees do not feel personally responsible for collaboration tool security.

Nearly one-third (30%) of employees state they would not feel personally responsible if an attack via collaboration tools were to occur and it involved their device/account.

A lack of monitoring can be dangerous.

Cybersecurity leaders are not monitoring employee use of these tools, nor treating this communication channel like the attack vector it has potential to become.

collaboration X tool X
security X is X more X
important X than X
ever X

The need for focused and comprehensive collaboration tool security is more important than ever.

This is where advanced [email security](#) has a critical role to play, providing the benefits of layered security and protecting organizations against a single point of attack entry. Organizations need to seek out and implement advanced email security solutions that offer best-in-class protection against the most sophisticated attacks and can help keep messages and attachments secure not only on email but also on collaboration tools, catching what Microsoft 365 misses.

About these survey results

This quantitative research focuses on how employees and cybersecurity leaders are responding to the rise in the use of collaboration tools in the workplace – analyzing their habits around, and understanding of, using email and collaboration tools in a hybrid world. We spoke with more than 3,000 employees and 600 cybersecurity leaders, 53% of whom are CISOs, CIOs, and CTOs, and 47% of which are IT directors. Survey respondents are from Australia, France, Germany, South Africa, U.K. and the U.S. Respondents represented sectors including financial services, entertainment, healthcare, public sector, and retail.

WORK PROTECTED.TM
Advanced Email & Collaboration Security

mimecast