freedom to focus

Securely empowered employees, protected businesses

distr

action

Foreword by:
Steven Bond, The Open University

Including contributions from:
Shira Rubinoff, leading cybersecurity advisor and author
Martin Veitch, IDG Connect

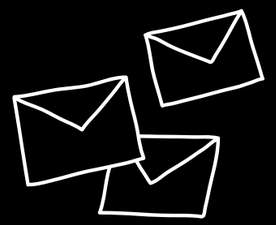
zivver

Contents

Research approach
In March 2022, we conducted interviews with:

- 6,031 employees who use email at work, from a range of job roles and sectors
- 855 IT decision makers who have responsibility or influence over data security in organizations with 250+ employees

Interviews were conducted across the US, the UK, the Netherlands, France, Germany, and Belgium by the specialist market research consultancy, Insight Avenue.



freedom

Expert contribution

Steven Bond
Information Rights Manager,
The Open University

Email. The first thought, the ‘go to’ communication tool and platform that allows flexibility in the workplace. Relatable?

Email. The business necessity. The mass communication tool. The method to get your point across without interruption, the chaser when something gets missed.

You attach a document. You hit send. Easy huh? But then you realise it’s the wrong document, or the wrong recipient. You’re now in a situation where you have breached security – something that can have serious repercussions – financially, legally and to your business’ reputation. Given that email is ‘person-centric’, it is a significant risk platform when it comes to security, with most data breaches being a result of human error linked to email. Yet, it is one area that is often not prioritised by IT leaders who instead focus more on inbound security. With so many other collaboration tools in use these days, mostly with the intent to help, not hinder, we’re experiencing a communication overload. This creates potential confusion as well as lost time and productivity as we try to learn these different platforms and decide which to use for which task, all while being continually interrupted. Often these tools are implemented with little guidance on which to use in what scenario, with email being the familiar ‘catch all’ that people revert to – the comfort blanket. But with comfort comes complacency, and the risk of a rogue attachment, or incorrect recipient rises.

How can email stop being a distraction and be the tool that it is hoped to be?

This report will explore the effect of data security training on the individual, and what leaders ‘think’ compared to what actually happens. We also explore the volume of tools and platforms available to users, and the impact that this can have on productivity and security, whilst recognizing the positive synergy that such can bring when integrated well.

There are mechanisms that can help the user to build trust in IT and their email system, moving away from a ‘people problem’ towards an IT solution. Enter Zivver.

As the hyper-acceleration of digital transformation and the proliferation of remote work continues, the need for employees to collaborate in real-time across digital channels is growing by the day. IT leaders have a key role to play in enabling this, empowering staff with the right tools and the freedom to focus without undue friction.

But with the number of data breaches rising by the year, they must also ensure robust security, creating an environment where rapid and continual communication doesn't lead to reputational damage or costly fines. So how can they get this balance between freedom and security right – and what tools or strategies will be critical to their success?

To find out, Zivver – a leader in secure communication solutions – commissioned one of the largest ever independent global surveys into secure digital communications and employee productivity. Explore the articles to follow how IT leaders, CISOs and DPOs can usher in a new age of secure and productive collaboration – including a quick snapshot of our key findings.

In March 2022, we conducted interviews with 6,031 employees who use email at work, from a range of job roles and sectors and 855 IT decision makers who have responsibility or influence over data security in organizations with 250+ employees.

Interviews were conducted across the US, the UK, the Netherlands, France, Germany, and Belgium by the specialist market research consultancy, **Insight Avenue**.

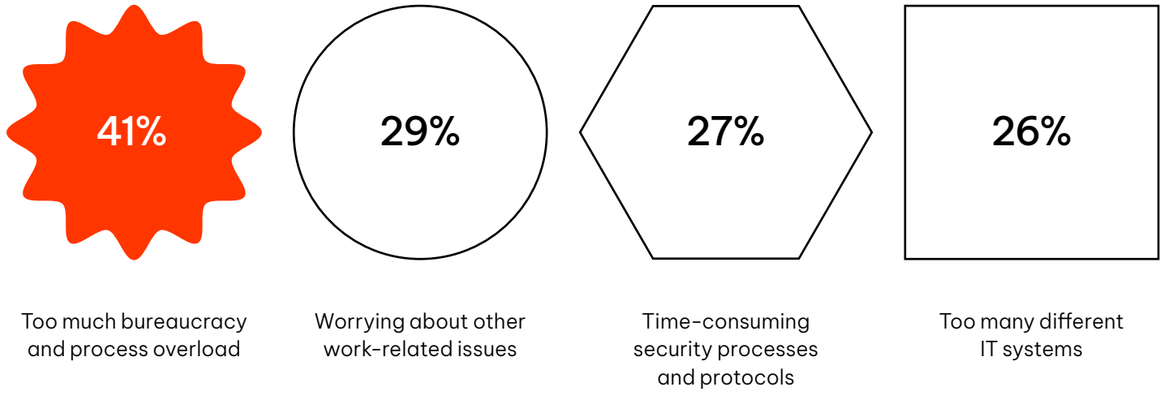
The snapshot

Barriers to focus in a changing workplace

Pitching a bold new marketing campaign. Crafting a killer sales deck for a new prospect. Implementing a smart new system to drive financial efficiency. Whatever the task at hand, employees produce the best possible outcomes when they feel empowered to make decisions and can concentrate fully on what they're doing. So it's no surprise that 98% of employees in our recent research agreed that it's important to be free to focus on their core role at work this year.

Yet today's workplaces are filled with distractions and friction, preventing employees from focusing on their most important work.

The biggest barriers to employees focusing on their core role at work



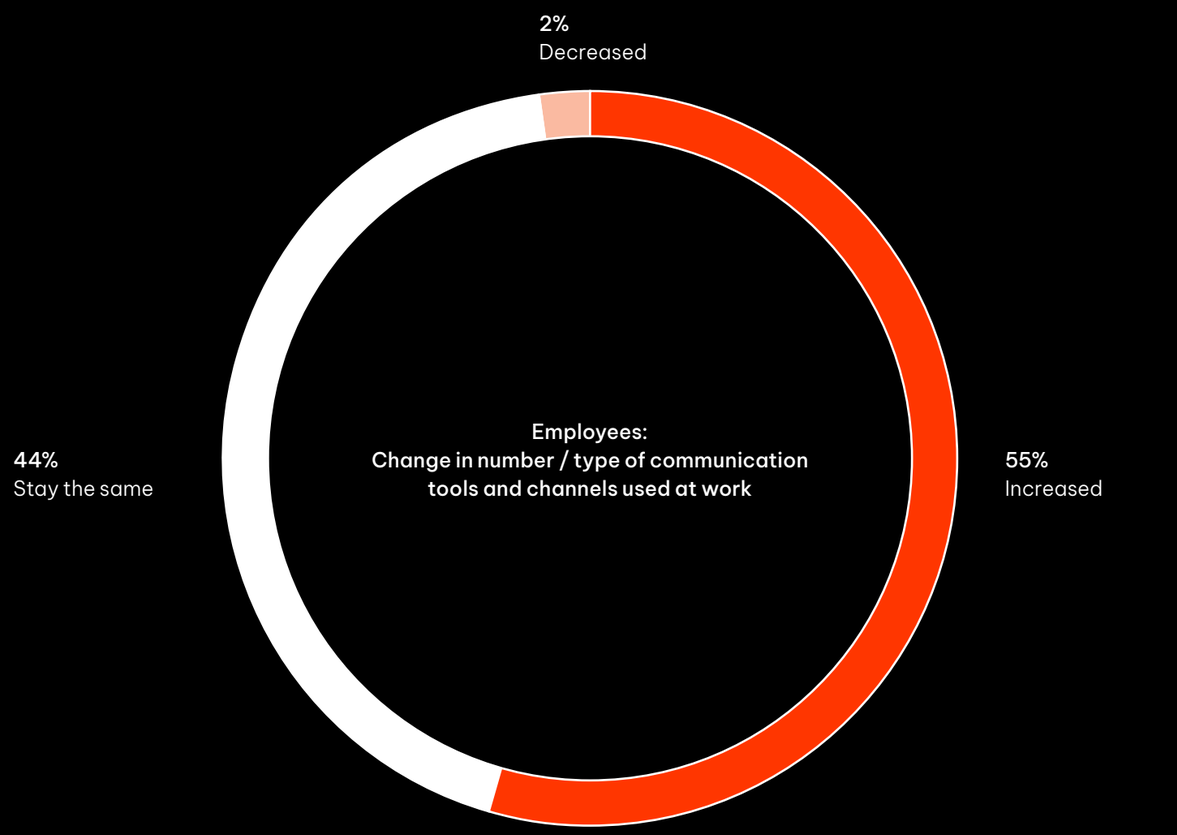
Too much bureaucracy and process overload

Worrying about other work-related issues

Time-consuming security processes and protocols

Too many different IT systems

Distractions have been exacerbated by remote working in the last two years: over half of employees (55%) have increased the number and type of tools they use to share information for work purposes.



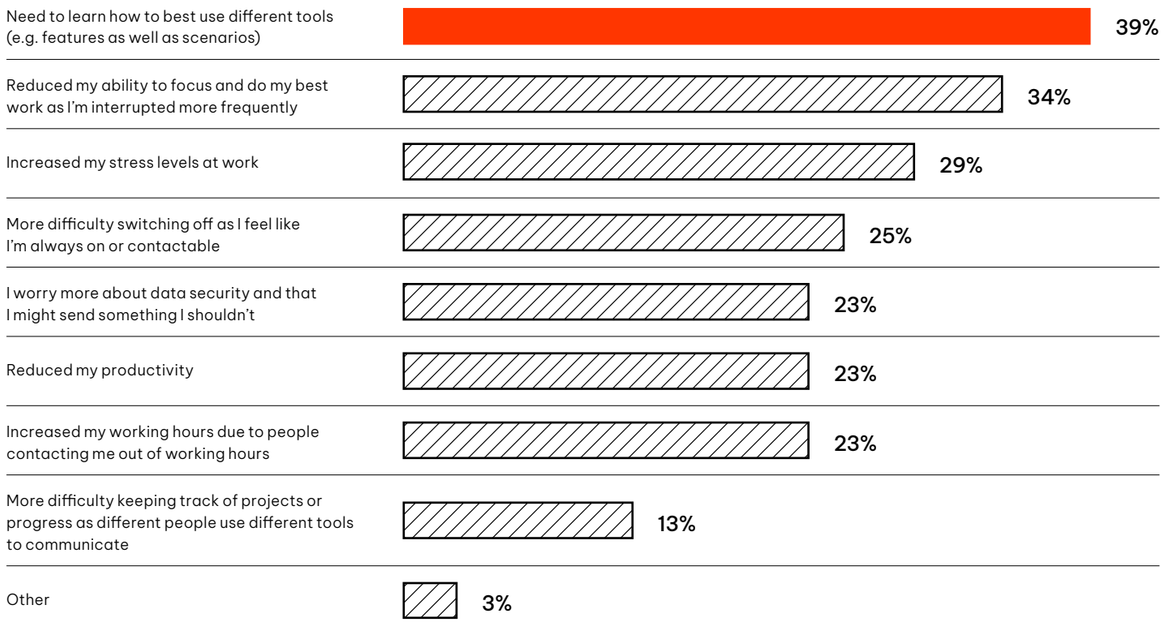
Regional snapshot		
% of employees who say the number and type of communication tools they use have increased in the last two years	UK: 57%	Germany: 50%
	US: 63%	France: 50%
	Netherlands: 52%	Belgium: 55%

More tools, more problems?

The result? A combination of collaborative noise and IT friction means employees are less able to focus, feel more stressed, and are even at greater risk of causing data security leaks.

That's not to say that using a range of collaboration tools is a bad thing; these platforms have been critical to ensuring business continuity during the pandemic. But there is a clear tension between employees' desire for the freedom to focus and the way they currently operate.

Employees: Personal impact of increase in number and type of collaboration tools at work



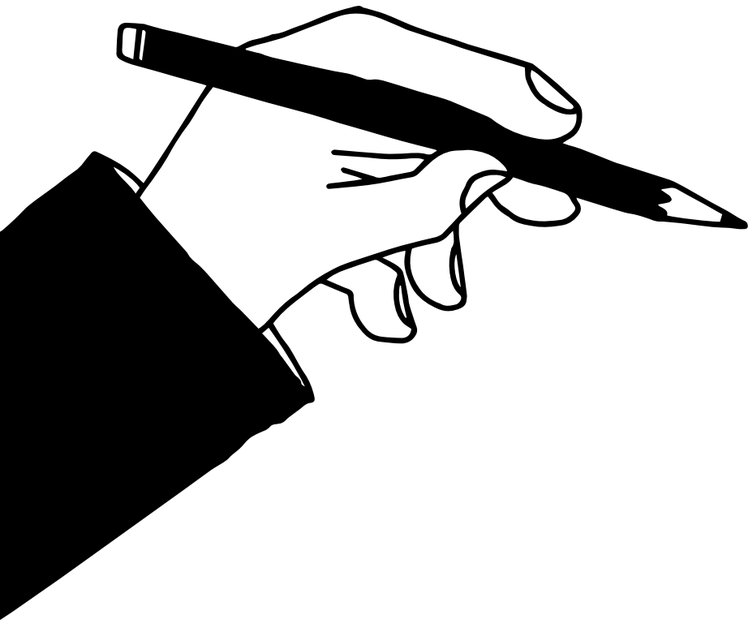
Regional snapshot		
% of employees who say an increasing number of tools has reduced their ability to focus and do their best work, as they're interrupted more frequently	UK: 30%	Germany: 38%
	US: 46%	France: 28%
	Netherlands: 31%	Belgium: 29%

The story in brief

While almost every employee wants to be free to focus on their core role, distractions like bureaucracy and time-consuming security processes are barriers to true focus. This problem is only growing as employees use more communication platforms to get their work done – which is leading to stress, and a greater risk of data security being breached.

Almost every employee wants to be free to focus on their core role.

Effective workplace communication: what tools, what risks?



Great work doesn't happen by chance. To create the best possible conditions for employee success, IT leaders need to implement tools, platforms and procedures that give every member of staff the freedom to focus, communicate freely, and even take a few risks now and again. (All while ensuring there's no *actual* data security risk to the business).

The first step to achieving that is understanding *how* employees are collaborating, sharing and communicating today.

Email is the most valuable channel – but it's not infallible

Instant messaging and video platforms have been in the spotlight over the last few years, but as it turns out, *email* is still the communication method most widely used by employees.

And employees don't just *use* email the most: they actively believe it's the most valuable and safest communication method. Nine in ten (88%) say they rely on email to get their job done, while 81% think email is the most secure way to send sensitive information.

> Overall, 88% of employees say they rely on email to get their job done. Almost all (97%) IT leaders say their organization relies on email as a business tool.

Employees: Methods of workplace communication most relied on by employees to get their job done

- 75% Email
- 49% Face to face/In person
- 43% Instant messaging
- 41% Video call
- 41% Phone

Regional snapshot		
% of employees who say they rely on email to get the job done	UK: 87%	Germany: 90%
	US: 87%	France: 86%
	Netherlands: 94%	Belgium: 86%

Just because something is familiar, doesn't mean it's safe

While employees like and trust email, it isn't foolproof from a business security perspective. There's a real risk that employees simply *presume* email is safe, because it feels familiar and useful – but that isn't necessarily the case. Messages can be intercepted once they have been sent. More understanding by IT leaders of applying semantic-aware, tailored secure encryption based on the sensitivity of content and detection of the recipient's security levels is key.

In addition, 62% of employees say they have made 'email errors' in the last two years, ranging from accidentally sending the wrong attachments to knowingly sending sensitive information that they probably shouldn't have.

Worryingly, employees are far more likely to make these errors when they're unable to focus. Elsewhere in our interviews, 45% of employees admitted that they have made risky decisions at work due to time constraints.

Email errors made by employees in the last two years

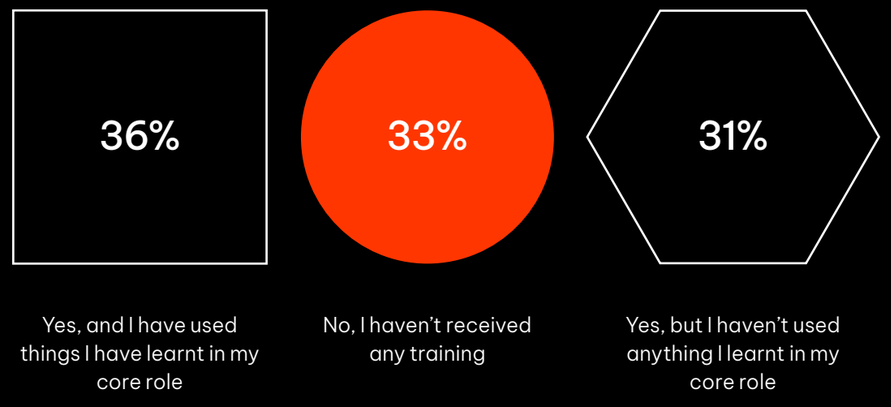
Situations where employees are most likely to make email mistakes

Rising risk, failing security measures

The **cost of data breaches is on the rise globally**, meaning there's real urgency for IT leaders to think carefully about how they tackle mounting security risks. Worryingly, many seem to be relying on behavioral training to protect their business: three quarters of IT leaders (76%) think that data security training alone will reduce email security mistakes.

But the reality is that this training is either failing, or non-existent. A third of employees don't think they've received any data security training – and of the 67% of employees that *have*, only 36% have actually used the things they learnt. For most organizations, data security training alone isn't enough to keep the business secure.

Employees: Data security training in last 12 months



Regional snapshot		
% of employees who say they have had data security training, but haven't used anything they learnt in their core role	UK: 38%	Germany: 33%
	US: 29%	France: 29%
	Netherlands: 32%	Belgium: 27%

Employees also lack faith in current security methods. Half say that ‘current security methods slow me down, and make me less productive’, while 39% think ‘IT teams are so paranoid about threats that it hampers me from doing my job’.

It all builds up to one clear picture: employees want the freedom to get on with their work, and email is a valuable tool in helping them achieve that. But email isn’t without risks – and current measures aren’t enough to protect businesses. There’s a real need for a smarter approach. Or, as 79% of employees agree:

It would be beneficial to everyone if there were a solution that protected people from email security errors.

The story in brief

Email is employees’ preferred method for communication at work, but many admit to making email security errors. Relying only on data security training isn’t a sufficient remedy; employees and IT leaders alike agree it would be beneficial if they had a smart technology solution that provided right-sized levels of digital security for email and helped prevented such errors.

Regional snapshot		
% of employees who think it would be beneficial to everyone if there were a solution that protected people from email security errors	UK: 84%	Germany: 78%
	US: 85%	France: 75%
	Netherlands: 78%	Belgium: 77%

king of comms

Email needs to fix security to prosper for another 50 years

Martin Veitch
Freelance Writer,
Analyst and Contributing
Editor at IDG Connect

To paraphrase Mark Twain's famous line, rumors of the death of email have been exaggerated for many years. Slate magazine published an article on '**The Death of Email**' in 2007 and in 2011 The Independent newspaper in the UK asked the leading question, '**Are we facing the death of email?**' And yet email is over 50 years old and continues to be used by billions of people. But, in order for email to survive and thrive for another 50 years, we need to fix security.

The fact is, as this new research from Zivver makes clear, email isn't going away anytime soon. This, it seems to me, is where we are today: email continues to be highly relevant and we think of it as auditable, formal, relatively non-intrusive... a medium that can be retained, searched and archived. Email has been around since before CDs, punk rock or VCRs but that doesn't mean that it's unassailable. And the biggest challenge it faces is security.

Email, like any asset, needs protecting and it is worrying that it remains a critical vector for attempted compromises from malware and phishing to ransomware and beyond. Email-borne exploits can be traumatic, expensive and hugely damaging to reputations. And, as rules such as GDPR become more stringent and carry heavier penalties, we all know that secure operations are fundamental to the running of a company.

Many of us have sent the wrong attachment in an email, accidentally hit 'reply all' or (the horror!) sent an email to someone we shouldn't have done, even if not everyone confesses to that. So, we need defenses to protect against our own failings as well as the aggressive actions of others. Ultimately, we need strong processes, education and training but also we need to rely more on automation and smart systems that can detect anomalies and check on actions. If I am sending an email with an attachment containing financial projections to a recipient not in my address book then that needs to be checked and validated.

Many CIOs and CISOs report that attacks have increased over the past two years as attackers have sought to take advantage of rapidly re-engineered processes, vulnerable home endpoints and networks.

Also, as this research shows, many firms are long overdue a security review. There will be no going back to the pre-pandemic world for many of us in the knowledge-working world. In fact, we need to reconstruct how security works in a hybrid-working world where most of us will spend much of our time not protected behind corporate firewalls but highly dependent on communications infrastructures.
IT is already stretched in a thousand ways and not every organization can field a crack SecOps team. We need smart tools that are non-intrusive and don't slow us down but protect us anyway, building confidence in our people that they are protected and safe.

Speaking to CIOs, CTOs and CISOs (by email!) the overwhelming impression I received is that most large organizations will use a cocktail of models to share information, views and news. But what they all stress is the need for security and governance. Says a veteran CIO: "If I want something to be on the record, I will email ... but I need to know that that email is safe and secure."

A CTO adds: "Email says 'this is probably fairly important and I might want to go back to it' [and] I don't have that feeling with Teams or Zoom. But for email to continue to be relevant it can't be seen as the wide-open transmission vector for threats."

A CISO says: "I recently attended a conference where an IT change executive said he was 'on a mission to stamp out email' because there were faster media. But if I know email is secure and auditable then I can count on it in a way that I can't with a Slack channel, IM or PM. That's why I think email will go on and on: if you protect it adequately and respect the risks, it just works."

The same goes for me as a writer: if I want a fast quote for a story, I will probably do what I did today to write this piece: send an email to a bunch of relevant people. Seven years ago, I sent an email to set up a **meeting with Ray Tomlinson**, who invented what we now think of as email. This informal hierarchy has been built into me for decades: I think most of us know when a medium is appropriate or otherwise and email is still valid for lots of things we need to achieve. But the faith we have in email erodes if we question its security.

Attitudes to email are moving in line with most technological shifts and that is more like evolution than revolution. We can observe an edging from one approach to another, but we can also expect long periods of coexistence. Email is still delivering the goods and, so long as we continue to sand down its rough edges and keep it secure, then it could yet live to be 100.

The communication risk landscape today: challenges for IT leaders

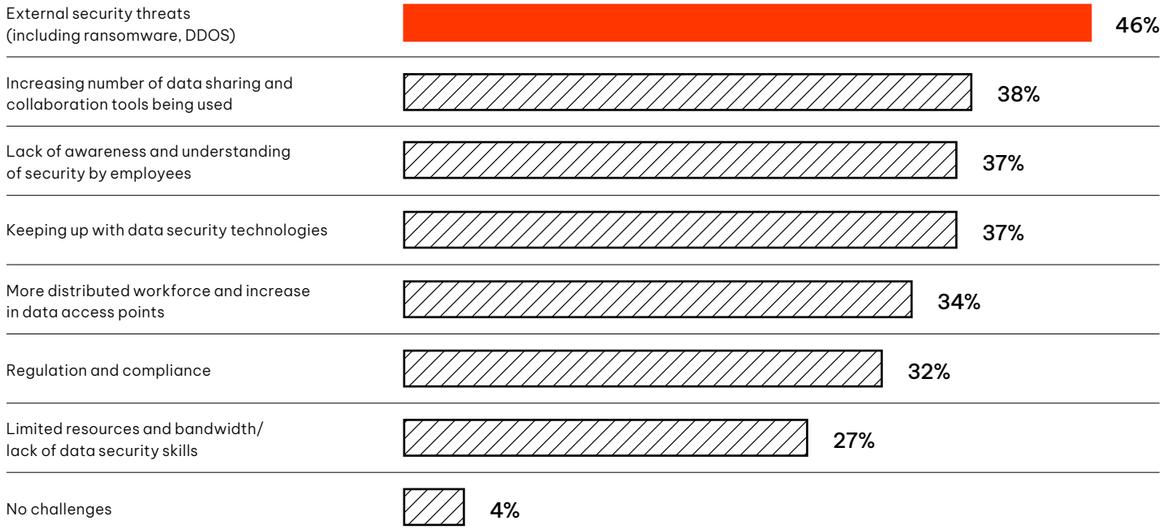
There's huge value in giving employees the freedom to focus and take calculated risks. However, as IT leaders know all too well, that freedom can't come at the expense of security and governance.

To tread the line between freedom and risk effectively, it's helpful for IT leaders to understand the communication risk landscape today.

What are the key data security challenges today?

External security threats (46%) are the most widely experienced problem, but a proliferation of data sharing or collaboration tools is another big issue (38%) – as is a lack of understanding about security (37%) and keeping up with data security technologies (37%).

IT: Key data security challenges



Upping the focus on outbound

IT leaders understandably place a great deal of focus on the threat of malware and phishing. But 'data loss through employee email errors' is almost as big a concern (43%), indicating that IT leaders need to think as much about outbound security failures as they do about external threats.

IT: Security threats organizations are most concerned about

48% Malware

46% Phishing

43% Data loss through employee email errors

41% Ransomware

40% Cloud computing vulnerabilities

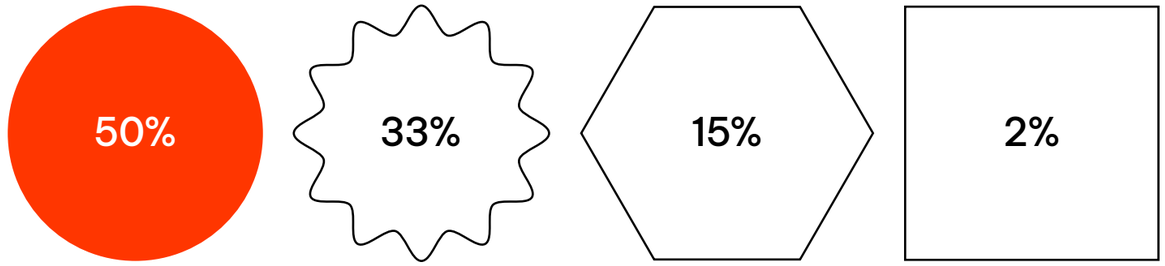
31% Advanced Persistent Threats (APT)

Regional snapshot		
% of IT leaders who say data loss through employee email error is the security threat they're most concerned about	UK: 50%	Germany: 37%
	US: 45%	France: 42%
	Netherlands: 35%	Belgium: 37%

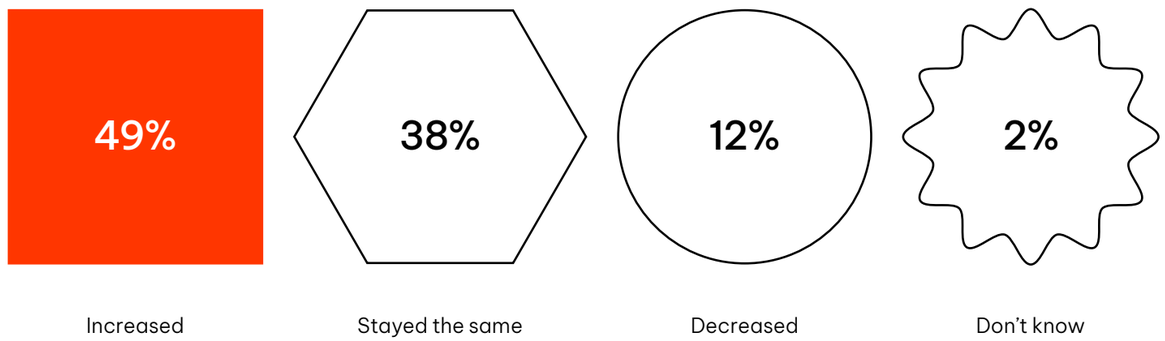
Keeping up with mounting risk

These risks are only growing. Half of IT leaders (49%) say 'external threats such as phishing or malware through links sent in email' have increased in the last two years, while 33% think there are more incidents of 'data loss through employees sending the wrong attachment in emails'.

Data loss through employees sending the wrong attachments in emails



External threats such as phishing or malware through links sent in email

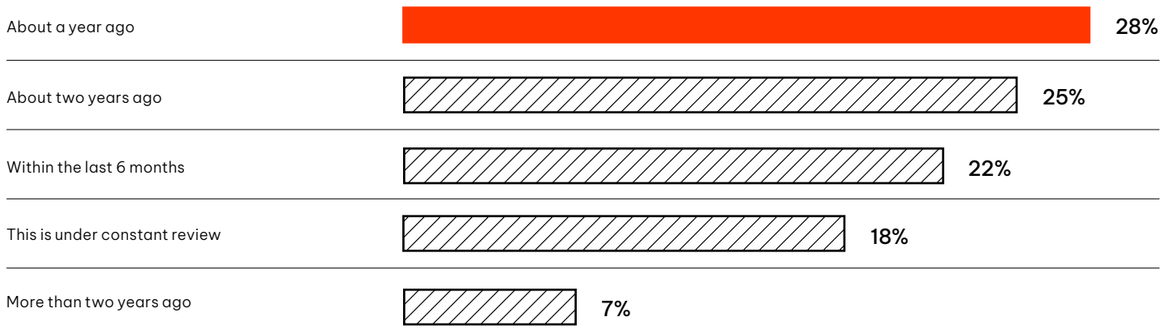


Trying to stay proactively progressive

Yet despite the constantly evolving nature of risk – and the growing problem of email errors or threats – many IT teams aren't regularly reviewing data security. Only 18% of IT leaders have their approach to risk and email security under constant review. Almost a third of IT teams (32%) last reviewed their approach to risk and email security two years ago or more. Given how much and how fast the world of work has changed, a more proactive approach is vital.

Data security training alone doesn't work, a strategy rooted in adopting progressive risk management with smarter technology could instead be the answer. Training people will always be important – but technology can take on a bigger role in preventing data leaks, empowering employees across the business to work securely and without disruption.

IT: When organizations last reviewed their approach to risk and email security



Regional snapshot		
% of IT leaders who say they reviewed their approach to risk and email security two years ago or more than two years ago	UK: 29%	Germany: 32%
	US: 23%	France: 50%
	Netherlands: 38%	Belgium: 18%

The story in brief

IT leaders face a range of evolving security risks, but external threats aren't the only problem. Data loss through employee email errors is almost as big a concern as malware and phishing. However, most IT leaders aren't keeping their security under constant review, putting them at risk in a fast-moving threat landscape.

Data loss through email is a big concern.

Shira Rubinoff
Cybersecurity Executive,
Advisor & Author

focus

As our world continues to be increasingly affected and run by technology, we find ourselves in a time when tasks are streamlined because of, and through, technological advancements, but also burdened by the sheer volume of apps, options, and platforms that we are now operating in. When it comes to business productivity, often workflows can get bogged or slowed down, employees can lose focus, and data security, especially an organization's outbound digital security, can be compromised. How do most people work or want to work, and what is best for an organization – vis a vis both productivity and, perhaps even more importantly, outbound security?

Zivver's recent research has brought up an interesting theme – is it true, as their results attest, that the more freedom an employee is given to focus, along with the tools and technologies to assist in that endeavor, the greater outbound digital security and protection for the business? Accepting that premise, why is that so, and what does it all mean?

In our ever-evolving world of technology, innovation and increasingly complex modes of communication, the time spent simply focusing on each action we have decreases both in quantity and quality. As humans, we are only equipped with a certain attention span, and given the increasing demands of the workplace, as we grapple to both absorb and learn more technologies, while producing more, especially in the COVID-19 and now almost post-pandemic era, something is bound to give. In many cases, that something is security, which can spell untold damage to any organization, particularly as it relates to outbound digital security.

Why focus on email?

The Zivver research demonstrated that over 85% of all employees polled in each of the market areas, rely on email to get their jobs done. 97% of the IT security professionals questioned say that email is one of the most important business tools used within their organizations. All believe that it is also the most secure way to share sensitive information. But in actual fact, mistakes by employees cause 80-90% of all data leaks. This is what happens when an employee is overwhelmed by technology and application overload, time constraints, production demands and general fatigue. With email playing such a critical role in business operations, and hack attacks through email on the rise, including malware and phishing, which 2/3 of the IT leaders polled report having experienced within the past two years, not to mention data lost or breached through employee human error, when it comes to better security, email is a good place to start.

The study determined that both external cyber threats and internal employee error and mishaps are increasing. Honing in on the human factor, Zivver proved that much of the escalation may be attributed to a lack of optimal focus and concentration by employees, which, in turn, is the result of technological inefficiencies, such as the over-abundance of and confusion surrounding multiple platforms needed to conduct one's work and too many different modes of communication. Since email appears to be the constant in all polls, by focusing on it as an area for a targeted review of the security technology available to work harder for individuals, an honest appraisal of where security training is or is not working, upgrades, and support, organizations may begin to realize elevated success in relatively short order.

To date, a mere 18% of IT leaders say that they regularly review their approach for risk and email security, with almost a full third admitting that their last review took place at least two years ago, in some cases, much longer than that. Wouldn't a more proactive approach be appropriate given the rapid pace of technological evolution and social change our world is experiencing?

And what about the everyday employee's end of things? The poll also revealed that given the overload already shouldered by employees everywhere, it would be impractical, as well as unrealistic and unfair to expect that people attend new and more training sessions, and adopt even more new protocols. To better streamline workflows and production processes for all employees, while also amping up organizational data security, particularly on the outbound end, all roads point to new technology tools.

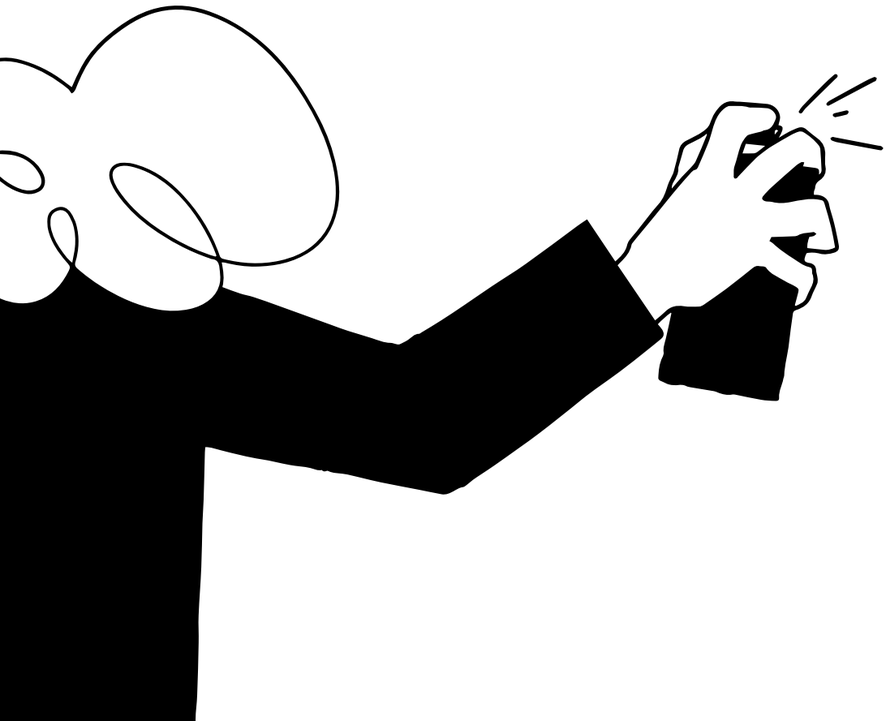
By supporting employees through a balanced and proactive risk management approach, coupled with comprehensive new innovations like smart technology, businesses will be able to consolidate processes and communications, and provide employees with the ability to perform better, in less time, and with greater focus. That, in turn, will also alleviate the pressure that contributes to human error, thereby also protecting businesses from any internal security threats that exist.

More focused employees will yield a more secure and productive business, and isn't that what both employees and owners alike really want?

Enabling progressive risk management with smart technology

Employees want the freedom to focus. IT leaders need to ensure that data security remains robust. The good news? There doesn't have to be tension between these two stances.

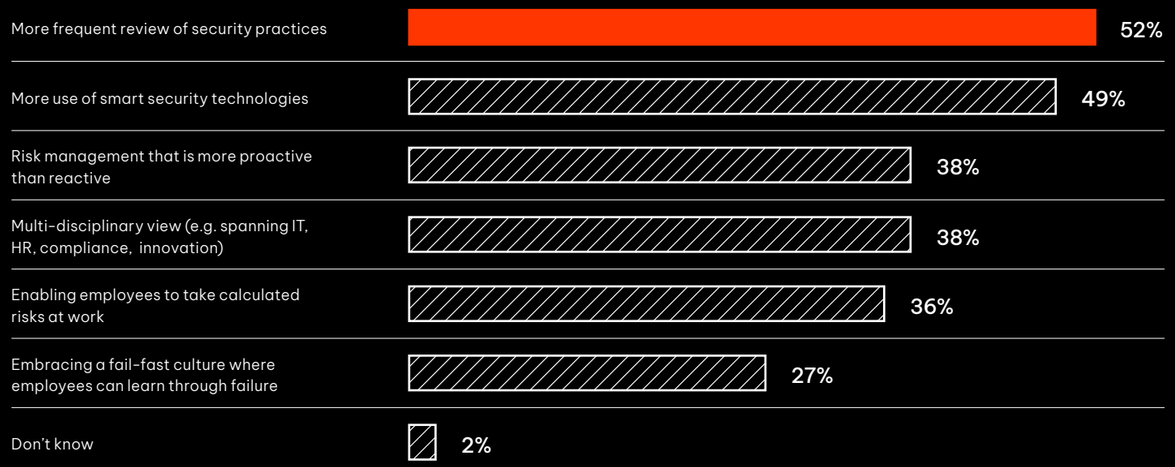
With the right technology and a more progressive risk management approach, IT leaders can set people free to focus on what really matters, all while protecting the business and its data. Fortunately, most IT leaders are already on board with making this shift.



In terms of what 'progressive risk management' actually looks like, it involves a mixture of behavioral-based strategies and smarter technology. Just over half (52%) of IT leaders say it means doing more frequent reviews of security practices, while 49% say it involves more use of smart security technologies (49%).

> Almost all IT staff (91%) think they could be more progressive in managing risk.

IT: What progressive risk management looks like



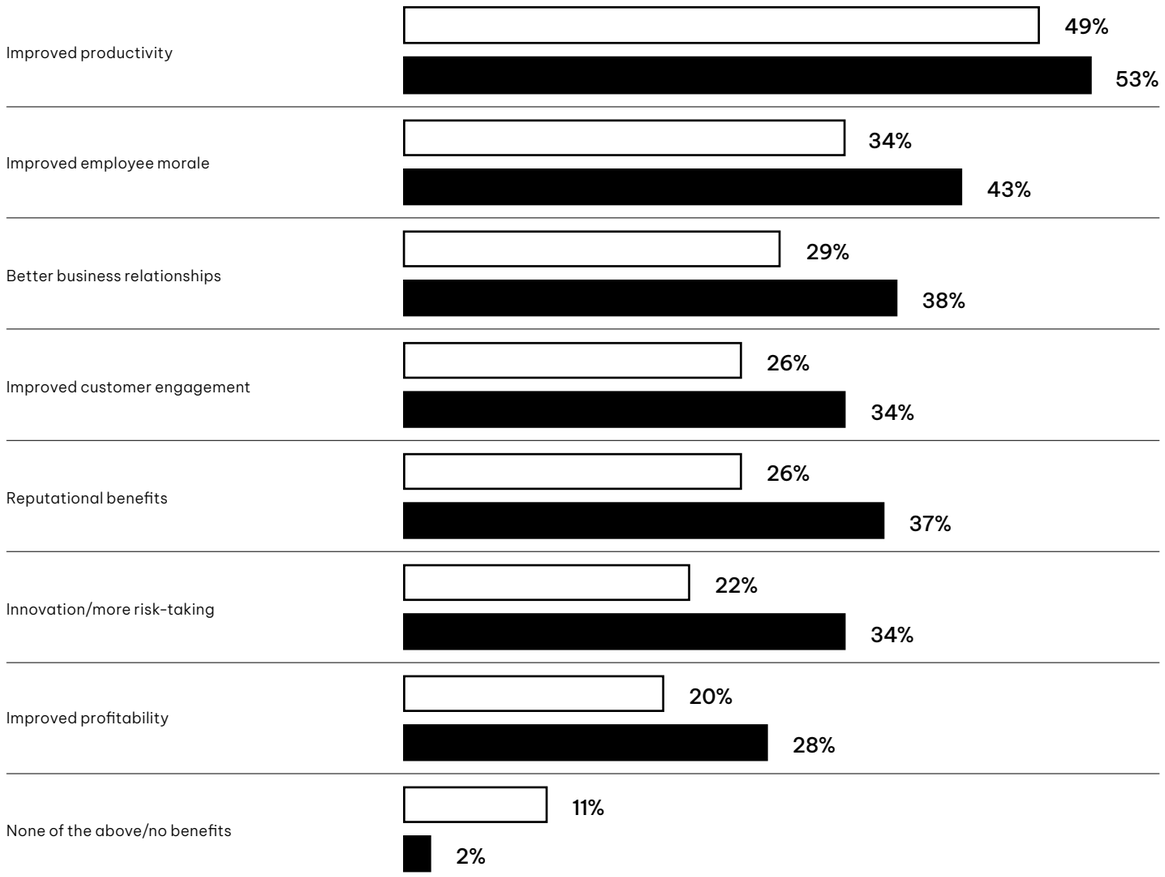
Technology as the path towards progressive risk management

Rather than treating email security risk as a behavioral problem, four in five (79%) IT leaders now think that smarter email data security could reduce errors, and 87% say it would be beneficial if businesses had a solution that protected people from email security errors.

In other words: IT leaders now understand that employees need tools and technologies that enable them to work freely, rather than more restrictive measures or processes. Accordingly, 73% of IT teams plan to invest more in outbound email security in the next two years.

As we saw earlier in this report, employees identify email as their key tool for communication and collaboration, even in an age of instant messaging and video conferencing – so this would be a positive step for many businesses to take. And, as the final graph of our research shows, both employees and IT think they would enjoy a range of benefits if they never had to worry about data security when using email.

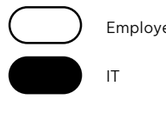
Employees & IT: Benefits if an organization invested in tech that meant never worrying about data security when using email, giving freedom to focus on other things



The story in brief

As it becomes clear that data security training alone can't protect businesses, many IT leaders are exploring progressive risk security strategies. Smart technology is increasingly being seen as the answer, rather than burdening employees with more security protocols and policies.

IT leaders are exploring progressive risk security strategies.



The secure future of digital communication

In a world moving so fast, employees must be empowered to work without unnecessary IT friction, which means moving away from unwieldy security protocols. But in a workplace so full of distractions, it's unrealistic to rely on data security training alone to keep the business safe.

Today's smart technology and a proactive risk management approach can provide the answer, ushering in a new age of secure digital communication. With that in place, the business stays secure, productive and fluid – and employees get what they want above all else...

...the freedom to focus on the work that really matters.

zivver

To find out more about how Zivver can help your organization to embrace the next generation of secure digital communications, please visit zivver.com