

kaspersky



Gen AI Business Infiltration:

C-Level executives are sitting on an AI timebomb, aware of the risks, but too complacent to act.

The C-Suite might well be sleepwalking into a generative artificial intelligence induced cyber security nightmare, allowing the transformational opportunities to blind them to the risks.

A Kaspersky Report
October 2023

Contents

Overview:.....	2
Methodology:.....	3
What we found:.....	3
- The not-so-secret Gen AI takeover	5
- So, who are the biggest Gen AI adopters?	6
- Fearing the Gen AI unknown.	6
- The boardroom debate.....	6
- Will action be taken?	7
- The future of Gen AI in business	8



Similar to BYOD, Gen AI brings the potential for increased productivity and a new way of working, but also raises serious concerns around security and misuse.

Overview:

Generative Artificial Intelligence (Gen AI) has transformed itself from a passing novelty into a pervasive force in our lives. Such is its popularity, tools such as ChatGPT are now being used for a wide range of tasks, from the creation of dating profiles to drafting email content.

As a result, Gen AI tools and applications have quickly found their way into the workplace, with employees in a variety of different roles using them for a range of different professional purposes. The trend is reminiscent of 'bring your own device' (BYOD) to work, a trend which saw workers increasingly using personal devices in the office, regardless of company policies or security protocols.

Similar to BYOD, Gen AI brings the potential for increased productivity and a new way of working, but also raises serious concerns around security and misuse. As a result, business leaders are now having to grapple with the fundamentals of the technology to understand if the benefits outweigh the risks.

For it to work effectively, Gen AI relies on continuous learning and refinement through data inputs. The handling of the data being used to feed these platforms raises questions about data ownership, security, and confidentiality. This process of data sharing runs the risk of so-called 'reverse data leaks' whereby an employee might unwittingly divulge sensitive information such as compromising business data or sensitive financial details.

The following report examines the attitudes of C-suite executives towards the adoption of Gen AI within their organisations and its impact on the workforce. It delves into how the boardroom perceives Gen AI technology, as a means to gain a competitive advantage, as well as revealing concerns about the use of tools like ChatGPT which have not yet been covered by official protocols and guidelines.

Kaspersky, a global company with threat intelligence experts operating in every region, has leveraged its unique expertise to conduct extensive research on the topic of Gen AI business infiltration and strategies from a C Suite perspective to ensure that businesses can continue to benefit from this transformational technology without risk.

Gen AI Business Infiltration: C-Level executives are sitting on an AI timebomb, aware of the risks, but too complacent to act.

1,863 online surveys C-level executives

were conducted by Censuswide
across the same 8 countries

95%¹ of C-level respondents

said that they know that Gen AI tools
such as ChatGPT are currently being
used in some way in their company.



Methodology:

A total of 1,863 online surveys of C-level executives were conducted by Censuswide across eight countries in 2023 between 25.09.23 and 02.10.23 in the UK (258), France (251), Germany (250), Spain (252), Italy (251), Romania (200), Netherlands (201) and Greece (200). Respondents were asked about their understanding of Gen AI, whether they

had been using it over the past year, and if they fully understood how it is used within their organisations.

Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles.

What we found:

The majority of C-level executives believe that Gen AI has already infiltrated their organisations, with the technology now silently driving day-to-day operation...

- 95%¹ of C-level respondents said that they know that Gen AI tools such as ChatGPT are currently being used in some way in their company.
- Over half (53%) believe that Gen AI is now driving certain departments and running key tasks in stealth in the background.

Gen AI is now firmly on the map during board meetings, however most executives admit they are unsure of how it works, and many are concerned over the security of their company data and IP.

- 95%² said that Gen AI has been a boardroom discussion point for them over the last six months.
- 91%³ express a need for a deeper understanding of how it operates and where the data goes once inputted.
- Over half (59%)⁴ are currently concerned about the risks of employees inadvertently leaking sensitive information when using AI.

Gen AI Business Infiltration: C-Level executives are sitting on an AI timebomb, aware of the risks, but too complacent to act.

Despite these concerns, few organisations have put appropriate safeguards in place, and most are leaving themselves wide open to the acknowledged risks of using Gen AI.

- Only 22% have discussed putting rules in place to regulate the use of Gen AI in their organisations.
- Despite the risks, when asked which department they are most inclined to automate using Gen AI, 24% identified IT and cybersecurity.

In fact, most C-level executives have no plans to stop employees using Gen AI in the workplace.

- Just over a quarter (26%) are personally using Gen AI themselves and as a result have no plans to stop employees from doing the same.
- 25% are allowing employees to use it and currently have no concerns about how it is being used across the business.
- 1 in 16 (6%) senior executives don't care if Gen AI is used by employees or not within their organisation.

Many senior executives aren't even sure exactly which departments are using Gen AI tools the most and for which tasks but hold certain beliefs as to how it might be being used.

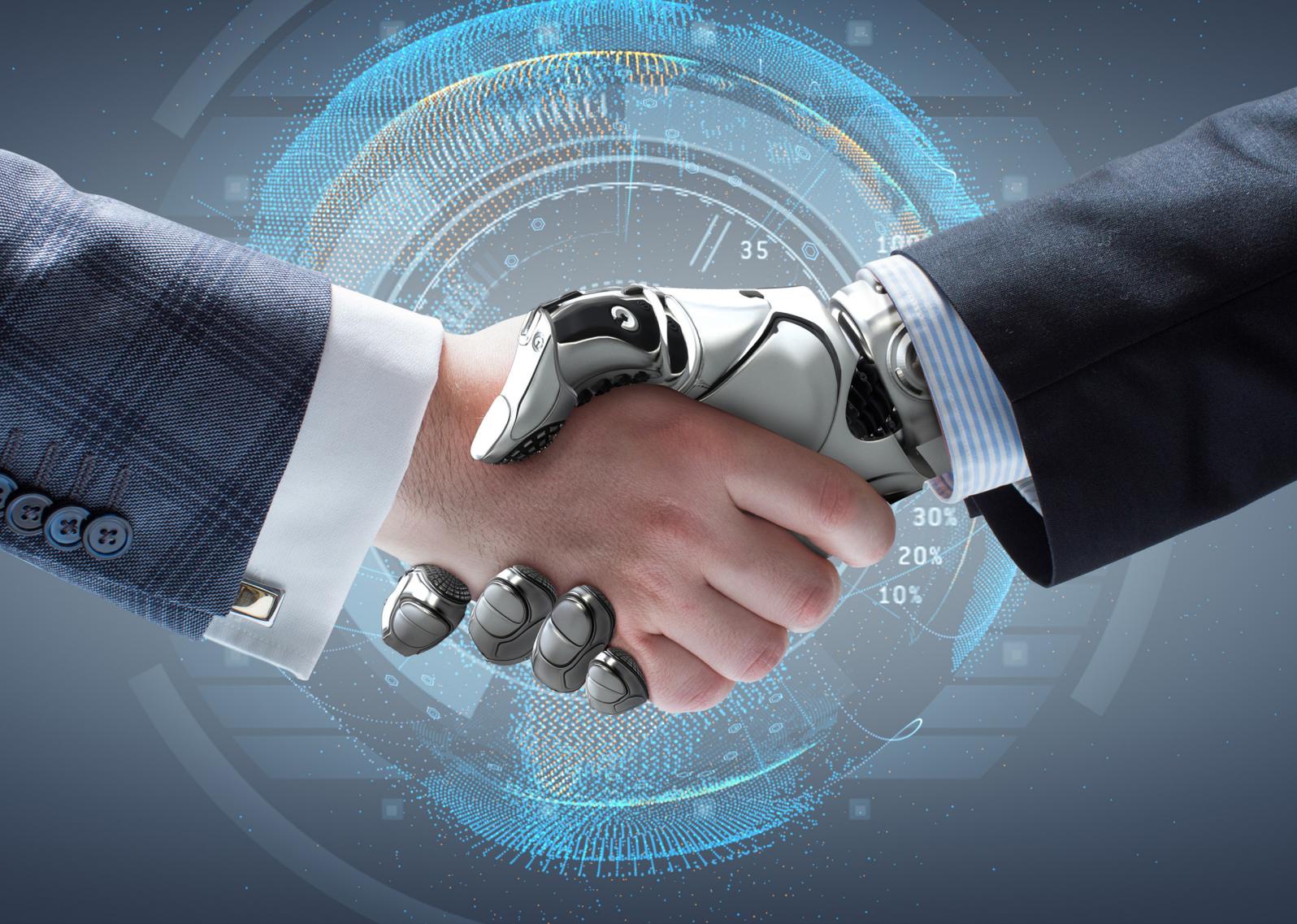
- Gen AI is most prevalent within IT departments (25%), then marketing teams (19%), followed by admin support (12%) such as PA's and executive assistants.
- There is a strong belief that tasks such as admin (49%) and day-to-day operations (41%) are the most outsourced tasks to Gen AI.

But despite major concerns and general lack of understanding around how the technology functions, C-level executives believe that the future of Gen AI in their organisations is bright. This all begs the question, are boardroom bosses about to hand over the keys to their kingdom, without the necessary protection to keep all their sensitive data safe...

- Exactly half (50%) say they are ready to leverage Gen AI to automate tedious task for their employees, and 44% intend to use it to speed up and simplify their own work.
- As well as everyday tasks, 40% also see it as a valuable tool for plugging the skills gap within their organisation, making it an instrumental asset in workforce development.
- 24% are keen to automate their IT and cyber security departments through Gen AI tools.



Over half (59%)⁴ are currently concerned about the risks of employees inadvertently leaking sensitive information when using AI.



The not-so-secret Gen AI takeover

“Time. It's the only thing you can't buy. I can buy anything I want, but I can't buy time.”

Warren Buffett

In both our professional and personal lives, time is one of the most precious commodities. We are constantly seeking ways to reclaim precious minutes and simplify routine tasks, allowing us to invest more time and energy into bigger picture priorities. Who wouldn't choose to delegate mundane daily chores if it meant more time could be unlocked for more important tasks?

Therefore, it's no surprise that Gen AI tools have surged in popularity over the past year. In the rapidly evolving tech landscape, the technology has made a significant impact not only with consumers, but also in the corporate world. But should more be being done to monitor and control its integration?

With almost all (95%)⁵ C-level executives acknowledging that Gen AI tools have been introduced into their corporate systems over the past nine months, and just over half (53%) admitting that they believe certain business operations are now being run in 'stealth' by employees through the technology, there still seems to be complacency around the risks.

Our research uncovers that, beyond clear security worries, the stealth integration of Gen AI is not a major concern, perhaps because more than a quarter (26%) of the C-suite admit that they themselves are personally using Gen AI to help with their own day to day jobs and therefore, right now, won't stop those who work for them from doing the same.

So, who are the biggest Gen AI adopters and what are they using it for?

While the boardroom cannot confirm with any certainty who is currently using Gen AI and for what purpose, there are certain departments which they believe are more likely to be using it than others.

According to the survey, the C-suite believes that IT departments (25%), marketing teams (19%), and administrative support (12%) which includes executive assistants, are among the most likely to be adopting Gen AI into their everyday processes. In addition, there is a suspicion that other key department such as sales (10%), HR (6%) and legal (4%) might also be using Gen AI to drive day-to-day tasks.

When asked what activities these departments are outsourcing to Gen AI, C-level respondents believed that everyday tasks such as generating basic content for emails (49%), are the most common, followed closely by activities aimed at streamlining day-to-day operations or finding efficient shortcuts (41%) which ultimately help speed up the completion of tasks on their to-do lists.



(91%)³ stating that they need a much deeper understanding of how Gen AI works and where their data goes once it is inputted into their systems.

Fearing the Gen AI unknown

Despite the rapid adoption of Gen AI, there is clear concern over the risks with just under 3 in 5 (59%) respondents stating that they are “very concerned⁴” that employees could disclose sensitive company information while using the technology.

Additionally, 57%⁴ expressed apprehension over employees taking shortcuts and data falling into the wrong hands, with the majority (91%)³ stating that they need a much deeper understanding of how Gen AI works and where their data goes once it is inputted into their systems.

Other boardroom worries include:

- Over half (54%)⁴ are concerned about employing people who have used Gen AI to bolster their CV and aren't as good as they appear on paper.
- 58%⁴ are worried about any sensitive information being leaked.
- 49%⁴ said that they fear losing competitive advantage and 55%⁴ their employee creativity as a people rely on the technology to produce their work.

The boardroom debate

Executive concern over usage has firmly installed Gen AI on the boardroom agenda but our research has found that few are discussing it in a way that reflects proper concern or the appropriate level of urgency.

and where the data goes once inputted, only 22% said they had discussed putting rules and regulations in place. Alarming, just under 1 in 7 (13%) felt that Gen AI had taken up more time than it should in their discussion.

Whilst 91%³ express a need for a deeper understanding of how Gen AI operates

1 in 16 (6%) said that they don't care if Gen AI is used by employees or not within their organisation.



Will action be taken?

Gen AI is clearly a hot topic of conversation. The technology brings with it many benefits, but also, just as many concerns. Yet, despite the potential risks, a quarter (25%) of the C-suite state they are allowing employees to use it as they do. In addition, 1 in 16 (6%) said that they don't care if Gen AI is used by employees or not within their organisation.

New technology is infiltrating organisations at a rapid rate and there is a fear at boardroom level that those who are using it could be putting the company's security at risk. Yet few at a senior level are planning to regulate it, and many are not even tabling it as a serious discussion point.



David Emm

Principal Security Researcher
Global Research and Analysis
Team, Kaspersky

"It is evident that the C-suite recognises the potential of Gen AI within their organisation and incorporating it into their daily toolkit. However, this technology is working its way into vital departments, despite acknowledging that Gen AI technology is still in its early stages and there is a need for a deeper understanding of its operations and data flow.

"The pressing question arises: would these companies allow their core departments to be managed by unknown third parties outside their organisation? If the answer is no, then why is it acceptable to place such trust in Gen AI?"

"Gen AI tools heavily rely on data and require a constant input of new information, acquired through various means, such as web scraping or manual data entry. The primary concern lies in the whereabouts of this data and who ultimately gains access to it.

"Sales or IT departments may innocently input sensitive company data to expedite mundane tasks. However, the moment this data enters a Gen AI tool, it ventures beyond the confines of the business environment. Essentially, employees could unwittingly facilitate a 'reverse data leak', where, instead of hackers infiltrating systems to steal data, employees unintentionally release it to the world."

Gen AI Business Infiltration: C-Level executives are sitting on an AI timebomb, aware of the risks, but too complacent to act.



The future of Gen AI in business

44%
intending to
integrate it into
their own routines
to reduce admin.

So, what lies ahead for Gen AI within organisations?

Despite its current covert use across critical departments, the prevailing lack of technical comprehension and substantial concerns regarding data security, in addition to the need to maintain a competitive edge is seemingly outweighing the risks that Gen AI creates. As such, the C-suite has ambitious plans for the technology within their organisations in the not-so-distant future.

The findings show that despite having major concerns around Gen AI, exactly half of executives (50%) are still aiming to harness it to automate the mundane tasks their employees currently handle daily, whilst 44% intending to integrate it into their own routines to reduce admin.

Furthermore, 40% of the boardroom sees Gen AI as the solution to the current skill gaps within their organisations, positioning it as a pivotal asset for the future of workforce development.

Gen AI Business Infiltration: C-Level executives are sitting on an AI timebomb, aware of the risks, but too complacent to act.



“You can't trust what you don't understand”

John C. Maxwell

Gen AI clearly offers advantages in both our personal and professional lives, providing shortcuts to save time and remove mundane tasks from our to-do lists. However, it raises important questions about the costs and risks involved in its integration.

The 'bring your own device' (BYOD) trend was hailed as a game-changer for businesses and employees, allowing people to work on their preferred devices which boosted productivity and reduced IT costs. However, issues soon surfaced. Unsecured devices compromised network security, and IT lost control over enforcing policies and updates. These made devices more susceptible to loss or theft.

While Gen AI adoption is different from BYOD, it poses its own set of risks. The C-suite's acknowledgment of Gen AI's presence in their organisations without policies, protection, or deep understanding is troubling. Even more concerning is that a quarter of them are currently considering outsourcing IT and cybersecurity to the technology.

It's often said that you can't trust what you don't understand, and this is particularly relevant for Gen AI. While it offers numerous benefits, caution is crucial and education on Gen AI's potential and challenges is needed. For its business use, policies must be established to ensure it is used correctly and for the right purposes. Gen AI should be a time-saver, not a threat to the business itself.

While there are many positives to the current enthusiasm among C-suite executives regarding Gen AI and its potential for business applications, exercising appropriate caution is paramount. It's imperative that boardroom discussions evolve to address the changing landscape.

If there's a desire to delegate critical activities and functions to Gen AI, it is essential to gain a deeper understanding of data management, including what can and cannot be fed into these systems. This understanding should be complemented by comprehensive policies throughout the organisation.

¹ Inverse of 'I have banned it in the workplace' and 'None of the above'

² Inverse of 'not at all'

³ All of yes answers combined

⁴ 'Very concerned' and 'fairly concerned' combined

⁵ Inverse of 'N/A I do not know of GenAI tools being used in my company'



kaspersky

<https://www.kaspersky.com/partners/managed-service-provider>
<https://www.kaspersky.com/enterprise-security/services>
www.kaspersky.com/
www.securelist.com

© 2023 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owners