INSECURITY IN B2B DATA SECURITY

Perspectives from the Ipsos Business Insights Collective on what needs to evolve to keep companies safe

January 2025

Authors:
Anne Hunter
Kristyna Kanzler
Holly Lyke-Ho-Gland

KEY FINDINGS:

1. The right data security rules are in place, according to 70% of the leaders we spoke to. Executives recognize their companies are taking security seriously.

2. But 40% of leaders interviewed felt their company's data security training was only somewhat effective, suggesting that education and implementation remain a real problem.

3. While a quarter of Business Insights Collective leaders are extremely confident in their organization's ability to protect sensitive customer data from unauthorized access and breaches, the majority feel there is still more to be done.

4. AI security is an area of high concern for these business decision-makers.

INSECURITY IN B2B DATA SECURITY

Perspectives from the Ipsos Business Insights Collective on what needs to evolve to keep companies safe

As digital connections multiply and security risks expand, the challenge of safeguarding data has become a critical focal point for companies, demanding attention and action from industry leaders. New perspectives from the **Ipsos Business Insights Collective** reveal a concerning disconnect: while most business leaders believe their companies have adequate data security policies in place, **many are anxious about implementation and education**, and believe this problem could grow **more severe as AI solutions proliferate**. This report delves into the findings, exploring the perspectives of senior decision-makers on the evolving challenges of data privacy and security, and outlining the crucial steps organizations must take to fortify their defenses in the digital age.

Methodology

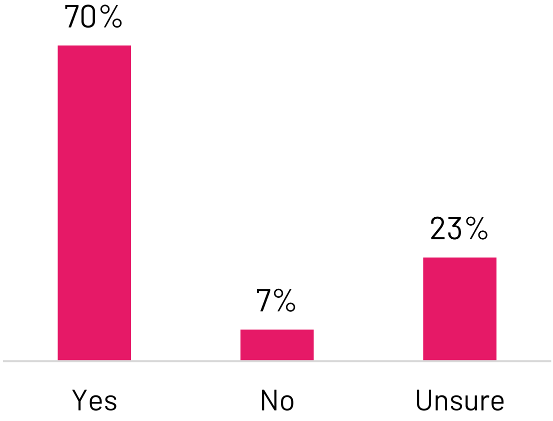
To better understand the latest perspectives in corporate data security, Ipsos Business Insights Collective was engaged. The Business Insights Collective uses the Ipsos Communities platform to gather business decision-makers across industries and seniority levels to discuss market-specific challenges and opportunities. Companies can drop in specific research questions, including text, video, or images, to get rapid feedback from their market of prospective customers.

An interactive discussion board with embedded qualitative survey questions was run in the Collective community space between September 24 and November 5, 2024. Ninety-four Collective members participated in the discussion board. This innovative format allows Collective members to answer questions with pre-set choices as well as expound on the topic in their own words and chat together about the issues, producing insights that go beyond standard quantitative data and provide the rationale for their opinions. In this study in particular, a gap emerged between how members rated their corporate security policies and their own personal concerns about their organization's security — something a survey alone would not uncover.

Business leaders think that their companies have the right policies

The good news? *Most* members of the Business Insights Collective feel their companies have built adequate rules and regulations to address evolving data security and privacy needs. A majority of senior leaders trust that security is taken seriously and understood by executives, who set the tone for all employees. **But this is no consensus: one in three Collective members is unconfident or unsure in the policies their companies have implemented.** It is critical for senior leaders, especially in technology departments, to understand where executives at their own company fall on this question so they can decide whether to maintain or adjust their current security initiatives.

Do you believe that your organization's rules and regulations are sufficient in addressing the evolving challenges of data privacy and security in the digital age?

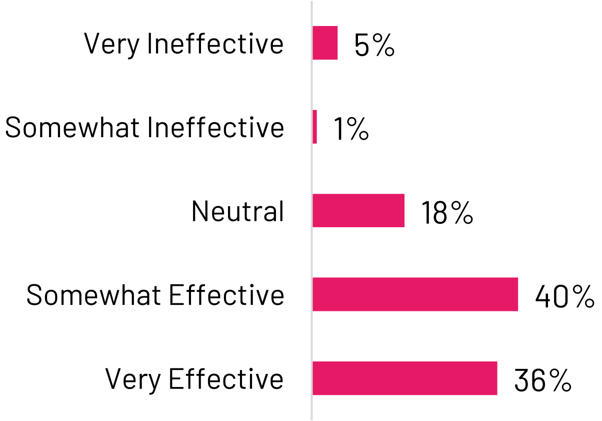


> *We have intelligence built into every aspect of our business to identify and lock down threats (and prevent threats). We have tools employees can use to report activity. We have a legislative/regulatory group that interfaces with the FCC and other groups. We also have a whole separate Cybersecurity division that we also offer as a service; that group helps our internal IT upgrade constantly to the latest security standards.*
>
> – Senior manager, enterprise media company

Training is key

Most members of the Collective feel that their companies have developed strong policies for data security. But keeping those policies up to date and ensuring that they're upheld by every employee in every circumstance is another story.

How effective are your organization's training programs in raising employee awareness about data privacy and security best practices?



Only 36% agreed that their training procedures were very effective at ensuring employees understood their organization's data security policies. **And in matters like data security, anything less than very effective is not good enough:** It only takes one mistake from one employee to cause a major data breach.

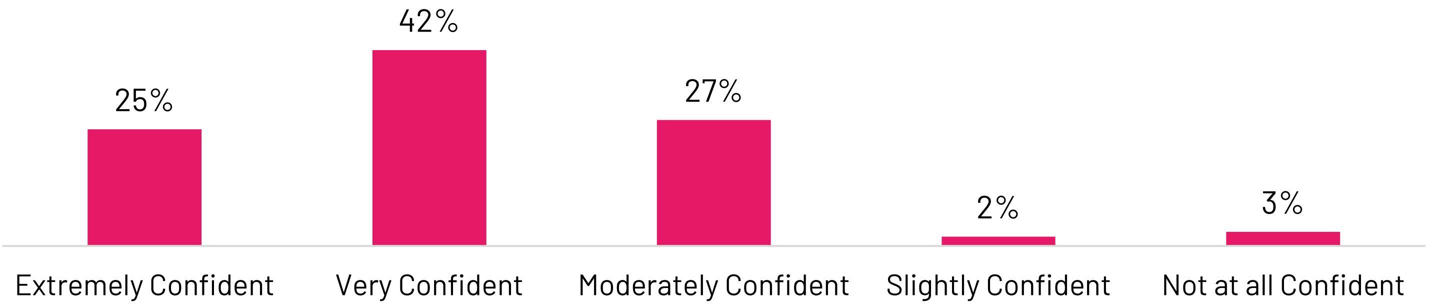
> *We have training, but it probably needs to be refreshed with the advent of new technology and threats.*
>
> – Senior leader, banking firm

> *We have a tendency to use third-party canned trainings that are only as good as the information being provided by the company. Unfortunately, sometimes I think we train for training's sake, and not for the actual opportunity to learn.*
>
> – Middle manager, financial services company

Access to sensitive data isn't universally locked down

Ensuring employees are well-trained is essential to protecting sensitive customer data. But when it comes to confidence in customer data security, the data belies a wider variety of perspectives among members of the Business Insights Collective.

How confident are you in your organization's ability to protect sensitive customer data from unauthorized access and breaches?



While 42% of Collective members said they were very confident**, the discussions around their experiences with customer data tell another story.** Often, people who said they were very confident, went on to describe **real concerns about customer data privacy**. This was particularly acute with people who worked in the healthcare industry.

> *Unfortunately, when it comes to healthcare, ironically paper medical records were MORE secure and private than today's electronic medical records. This is because paper records were static, heavy and could not be easily accessed by hackers.*
>
> – Senior manager, healthcare company

> *I'm at the mercy of the clinicians I contract with, so I don't have much say in what privacy or security measures they take for their clients.*
>
> – Owner, Healthcare consultancy

> *In most cases, when news is released of employees being fired for inappropriate access to medical records, it was because of the employee's failure to follow a well established and documented policy and procedure regarding access to medical records.*
>
> – Senior manager, healthcare firm

Employees' roles impact their perceptions

One striking finding is that executives' confidence in their company's security varies by **industry, seniority and department**. For example, while only 25% of Collective members were extremely confident in their companies' ability to protect sensitive customer data, **31% of Collective members who work in the finance and technology departments, have extreme confidence**. While this datapoint may inspire confidence, it has the potential to be a liability: finance and technology leaders know the detailed policies in place to keep customer data secure, but they may underestimate how the average employee might buck the policies the IT team so prudently developed.

> *The content covers essential topics, but the delivery often feels routine, which can lead to employees not retaining or applying the information as effectively as they should. Additionally, there isn't enough focus on real-world scenarios or ongoing reinforcement beyond the initial training sessions. To be truly effective, I believe the program needs to be more interactive and continuous, with regular updates to keep up with evolving security threats.*
>
> – Senior manager, technology firm

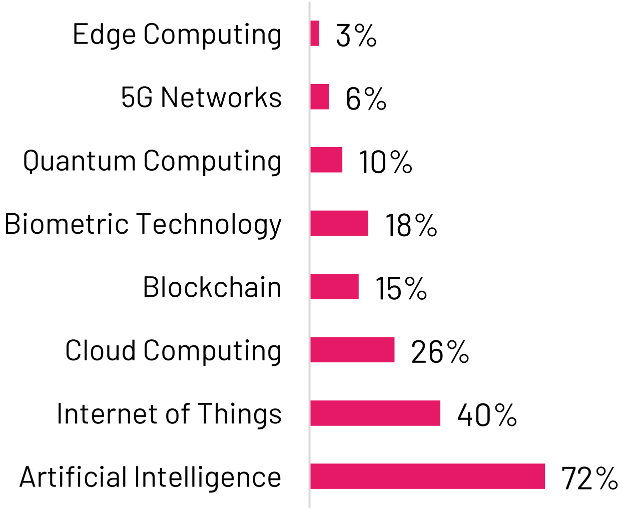
And while rank and file employees may feel they're on top of security, the c-suite feels otherwise. **38% of Business Insights Collective members with executive-level jobs had doubts about their company's ability to secure personal data —** ten points higher than the level of doubt among middle managers. Expectations remain high for IT leaders to keep customer data safe, in the face of ever-evolving threats and regulations.

> *Adapting to the evolving regulatory landscape surrounding data privacy and security is crucial for any organization.*
>
> – C-suite executive, manufacturing company

AI leads data security concerns

Of a range of emerging technologies, AI is the biggest worry for Business Insights Collective members, with **nearly three in four leaders** expressing concerns about its implications for data security.

Which of the following emerging technologies do you believe pose the greatest potential risk to data privacy in your industry?



> *AI is not quite reliable enough (yet?) to give it responsibility over sensitive information.*
>
> -Owner, small business

> *We are still at the early stage of AI which brings both the huge potential of improving end user productivities but also risk of data security.*
>
> -Senior manager, communications firm

> *I think all the AI and Cloud can protect the data but also can be a lever for the hackers at the same time.*
>
> -Senior manager, financial services company

5 Best Practices

Looking across the totality of the Business Insights Collective discussions on data security, and the resulting scores members give their own organizations, five key themes emerge as best practices.

1 **Regular Training and Education:** Regular training programs are crucial to keep employees updated on the latest data privacy regulations, best practices, and emerging threats. This includes mandatory training, ongoing education courses, and frequent meetings or workshops. Some organizations use a combination of in-house examples, external resources, and periodic testing to reinforce learning and assess employee understanding.

2 **Investment in Security Measures and Technology:** Organizations must invest in security measures such as encryption, access controls, data loss prevention tools, firewalls, multi-factor authentication, and VPNs. This also includes robust data governance frameworks and support from cybersecurity firms.

3 **Policy Reviews and Updates:** It's essential to regularly review and update data security policies and procedures. This includes aligning internal policies with evolving regulations like GDPR, CCPA, and HIPAA working closely with regulatory bodies, industry groups, and external consultants.

4 **AI Use Assessment, Education and Guidelines:** AI tools are infiltrating companies, whether they like it or not, through add-ons from existing vendors and individuals using consumer grade tools in their work. Having a robust AI governance and tools built for secure commercial applications while continuously educating staff at all levels on the proper use of AI is critical.

5 **Collaboration and Communication:** Open communication and collaboration were repeatedly highlighted as important aspects of adapting to the data security landscape. Some organizations encourage internal discussions and knowledge sharing among employees to foster a security-conscious culture. The action and importance given to data security by executives sets the tone for a culture where data security and privacy are taken seriously.

Join the conversation

Dive deeper into the perspectives of senior business leaders on data security or any other topic with the Business Insights Collective.

This group of leaders across industries and departments is always on to provide their opinions about business challenges such as:

- Market and buyer trends
- Message and content optimization
- Brand and competitor perceptions

With rapid feedback available in days, you no longer need to guess what the B2B market is thinking.

For additional information about engaging the community for your business needs, please contact **kristyna.kanzler@ipsos.com**

AUTHORS:

Anne Hunter
Senior Vice President, B2B Products and Go-to-Market, NA
anne.hunter@ipsos.com

Kristyna Kanzler
Vice President, Ipsos Communities
kristyna.kanzler@ipsos.com

Holly Lyke-Ho-Gland
Director, Ipsos Communities
holly.lyke-ho-gland@ipsos.com

Images by Ipsos Facto.

ABOUT IPSOS

At Ipsos we are passionately curious about people, markets, brands, and society. We deliver information and analysis that makes our complex world easier and faster to navigate and inspires our clients to make smarter decisions. With a strong presence in 90 countries, Ipsos employs more than 18,000 people and conducts research programs in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals.