IFF Research

AI Cyber Security Survey

Department for Science, Innovation and Technology

April 2024

Contents

1 Executive summary

Introduction

The Department for Science, Innovation and Technology (DSIT) commissioned IFF Research to conduct a survey of businesses in key sectors to understand how they use Artificial Intelligence (AI) and how businesses implement cyber security practices and processes around the AI technology they deploy.

The quantitative survey was developed in collaboration with DSIT. Fieldwork was conducted using Computer Assisted Telephone Interviewing (CATI) and took place between 10th January and 13th February 2024. A total of 350 interviews were completed with businesses currently using or considering using AI in nine sectors (see page 6 for more details) so that the survey had a robust number of participants.

The core objectives of the research were to understand:

- What types of technology are being used, and for what purpose;
- Businesses' cyber security practices – in general terms, and specific to AI;
- Businesses' future plans in relation to AI and cyber security; and
- How these activities and attitudes vary across businesses in different sectors and of different sizes.

A glossary which includes definitions of the different types of AI can be found in the Appendix at the end of this report.

Key findings

The survey sought to create a robust sample base of businesses that were adopting at least one AI technology as well as businesses that planned to adopt AI in the future to ensure robust findings could be drawn. 68% of these businesses in the survey were currently using at least one AI technology, while 32% had plans to adopt AI in the future. Of the businesses currently using AI, 64% were deploying one type of AI technology, 22% were using two types of AI and 14% were using three or more.

Among those currently using AI, natural language processing and generation was most common with 38% of businesses deploying it. 27% utilised machine learning, 25% used computer vision, image processing and generation, 9% used hardware related to AI and 8% used robotic process automation.

For each type of AI technology, over half of businesses have been using it for at least one year. In the case of machine learning, over half of businesses (52%) have been using it for over 3 years. Among those who have not yet deployed AI but have plans to do so, they most commonly planned to do this – across all AI technologies – in more than a year's time.

Each AI technology was most commonly adopted through the purchase of external software or ready-to-use systems (ranging from 38% to 60%). Around one in five businesses developed machine learning (21%) and hardware related to AI (19%) in-house. AI development most likely to be outsourced was for hardware related to AI (34%). The main reason cited for using AI technologies was financial or cost savings to their business (35%). 14% employed it to help write documents. 13% cited speed and efficiency purposes, and a further 12% used it for content generation more broadly.

Of those currently using AI technologies, nearly half of respondents (47%) had no specific cyber security practices in place specifically for AI and 13% were unsure. Among those planning to use AI in the future, 25% said that their organisation would not have specific cyber security practices or processes in place explicitly regarding the AI technology, once the planned technologies were deployed, and a further 25% were unsure.

Of those without or not intending to have specific AI cyber security practices or processes, there were a few key reasons as to why they had not adopted specific practices. 14% had not considered it or did not know enough about it, and 14% said they do not use AI for anything sensitive.

The survey also asked participants whether there were specific cyber security requirements or features that they expect to be built into AI companies' models and systems. 39% of respondents stated no and a significant minority (33%) were unsure.

When asked more generally about cyber security practices, 90% of all businesses had at least one governance or risk management arrangement in place. Just under three-quarters (72%) had a formal policy or policies in place covering cyber security risks, and around two-thirds had either a Business Continuity Plan that covers cyber security (67%), or a written list of the most critical data, systems or assets that their organisation wants to protect (64%).

Over the last 12 months, just over three-quarters (78%) of businesses had taken at least one measure in an effort to identify cyber security risk. The most common measures taken by organisations were to conduct a risk assessment covering cyber security risk (59%), or to invest in specific tools designed for security monitoring, such as Intrusion Detection Systems (55%).

2 Introduction

Background

The Department for Science, Innovation and Technology (DSIT) commissioned IFF Research to conduct a survey to understand how Artificial Intelligence (AI) is used by businesses in key sectors and how businesses implement cyber security practices and processes around the AI technology they deploy.

Artificial intelligence is the broader field encompassing knowledge-based systems, data-driven and machine learning-enabled systems, including classic machine learning (supervised learning, unsupervised learning), deep learning, and reinforcement learning, referring to the development of systems that can perform tasks requiring human intelligence. The use of AI is growing. In April 2023, an estimated 16% of all UK businesses had adopted at least one AI technology[1] and with the growth of more accessible and powerful generative AI models, this number is likely to increase significantly. The growing use of AI among businesses presents huge opportunities; however, without appropriate safeguards there are also significant risks. This is particularly the case with cyber security which is an essential precondition for the safety of AI systems. It was in this context that DSIT commissioned IFF Research to carry out primary research among UK businesses.

Research objectives

The core objectives of the research were to understand:

- What types of technology are being used, and for what purpose;
- Businesses' cyber security practices – in general terms, and specific to AI;
- Businesses' future plans in relation to AI and cyber security; and
- How these activities and attitudes vary across businesses in different sectors and of different sizes.

A glossary which includes definitions of the different types of AI can be found in the Appendix at the end of this report.

Survey fieldwork

This report is based on data from a quantitative telephone survey comprising of 350 interviews conducted between January and February 2024 with UK businesses currently using or considering using AI in the following sectors:

- D,E,H: Electricity, Gas and Air Conditioning Supply; Water Supply; Sewerage, Waste Management and Remediation Activities; Transportation and Storage
- C: Manufacturing
- G: Wholesale and Retail Trade
- J: Information and Communication
- K: Financial and Insurance Activities
- M: Professional, Scientific and Technical Activities
- Q: Human Health and Social Work Activities

[1] Understanding AI uptake and sentiment among people and businesses in the UK - Office for National Statistics (ons.gov.uk), June 2023

3 Methodology

A quantitative survey was developed in collaboration with DSIT and refined during a pilot fieldwork phase (full details of the methodology are included in the accompanying technical report). Interviews lasted an average of 15 minutes and fieldwork was conducted using Computer Assisted Telephone Interviewing (CATI) between 10th January and 13th February 2024 (inclusive of the pilot fieldwork phase). The interviewing team asked to speak to the person responsible for cyber security within the organisation.

Participants interviewed held a range of roles, often within the remit of IT or operations, such as: Head of IT, IT director / manager, Operations director / manager, Business development manager, and Office manager.

Sectors of interest and interview targets

This research sought to interview a total of 350 UK businesses, split equally among seven (grouped) sectors as shown in Table 3.1. The sectors were chosen by mapping SIC sectors where AI uptake is likely to be high, alongside Critical National Infrastructure sectors where the largest societal impacts from the exploitation of cyber security vulnerabilities are likely to exist.

Table 3.1 Interview targets by sector

Sector	Target
D,E,H: Electricity, Gas and Air Conditioning Supply; Water Supply; Sewerage, Waste Management and Remediation Activities; Transportation and Storage	50
C: Manufacturing	50
G: Wholesale and Retail Trade	50
J: Information and Communication	50
K: Financial and Insurance Activities	50
M: Professional, Scientific and Technical Activities	50
Q: Human Health and Social Work Activities	50

Sample

The sample for the survey was sourced from Market Location, a commercial database of UK businesses. The survey sought to create a robust sample base of businesses that were adopting at least one AI technology as well as businesses that planned to adopt AI in the future to ensure robust findings could be drawn. It was not possible to know at the point of drawing sample whether or not businesses were in-scope for the survey, therefore it was necessary to screen for this with a question at the point of recruitment.

Achieved interviews and response rate

Profile of participating businesses

A total of 350 interviews were achieved, split by size and sector in Table 3.2.

Table 3.2 Profile of participating businesses

Sector	Business size				
	Micro (1-9)	Small (10-49)	Medium (50-249)	Large (250+)	Total
D,E,H: Electricity, Gas and Air Conditioning Supply; Water Supply; Sewerage, Waste Management and Remediation Activities; Transportation and Storage	11	21	13	5	50
C: Manufacturing	18	16	8	8	50
G: Wholesale and Retail Trade	20	12	10	8	50
J: Information and Communication	23	18	6	3	50
K: Financial and Insurance Activities	27	15	4	4	50
M: Professional, Scientific and Technical Activities	23	11	11	5	50
Q: Human Health and Social Work Activities	14	17	9	10	50
Total	136	110	61	43	350

Call outcomes and survey response rate

A call outcome is defined as a definite response to the survey invitation, i.e. whether an interview was achieved, or whether an interview could not be achieved and the reason was established. Among the 10,924 businesses called at least once, the response rate for the survey was 3% (shown in Table 3.3). This included businesses where no final outcome was reached, for example where the interviewing team were not able to get through to the right person, where an appointment had been made to call back at a later date, or where a or where the call went to answerphone. Among the 2,193 businesses where a definite call outcome was achieved, the response rate was 16% (shown in Table 3.4).

10% of businesses screened out because they confirmed their organisation does not use AI and is not considering deploying it in the future. However, this proportion increases to 48% when based on records where a definitive outcome was reached. The high proportion of businesses screening out and subsequent lower response rate was expected due to the specific eligibility requirement of businesses needing to be using or have plans to use AI.

Table 3.3 Unadjusted response rate

	Number	%
Total records called at least once	**10,924**	**100%**
Completed	350	3%
Screen out - Organisation does not use AI and is not considering deploying AI in the future	1,059	10%
Respondent refusal	486	4%
Respondent unavailable during fieldwork	234	2%
Contact made – no definite outcome	2,707	25%
No direct contact made with respondent	5,056	46%
Over quota	64	1%
Unobtainable (e.g. wrong number, out of service)	968	9%

Table 3.4 Adjusted response rate based on a definitive call outcome

	Number	%
Definitive call outcome	**2,193**	**100%**
Completed	350	16%
Screen out - Organisation has not used AI and is not considering deploying AI in the future	1,059	48%
Respondent refusal	486	22%
Respondent unavailable during fieldwork	234	11%
Over quota	64	3%

Of the 350 businesses that took part in the survey, 239 were currently using AI. These businesses as a proportion of all those for whom we have a definite answer on whether or not they use AI, equates to 21%. This is slightly higher than the ONS finding in April 2023 which reported an estimated 16% of all UK businesses had adopted at least one AI technology.[2]

Reasons for not using AI

Respondents who confirmed during the survey that they do not use, or have plans to use, any Artificial Intelligence tools within the business were asked what has prevented their organisation from implementing AI technologies.

Among the 193 businesses who answered, the most common reason provided was that they have not identified a need for AI, including deeming it irrelevant for their sector or industry (44%). One in ten said they have not thought about AI or do not know enough about it (10%) and they have no interest in it, for example preferring human interaction (9%). 8% deemed AI unnecessary due to the small size of their business, 6% said they lack the time or resources to set it up and 6% had concerns about the security of AI models and systems, including data security and confidentiality.

Data analysis and weighting

Large and medium-sized businesses are over-represented in this survey compared to the business population. This was a deliberate decision - the Department needed a good-sized sample base of these types of businesses. Weighting by size and sector was therefore considered. However, as the

[2] Understanding AI uptake and sentiment among people and businesses in the UK - Office for National Statistics (ons.gov.uk), June 2023

number of interviews is small, the weights were deemed too large to apply and would have had a considerable negative impact on the effective base size. Specifically, it would have meant that it would not be possible to report the findings of businesses of a particular size or sector. These survey results cannot therefore be considered representative of the business population, however, can still provide useful insight into the behaviour of businesses that took part.

4 AI usage

This chapter explores:

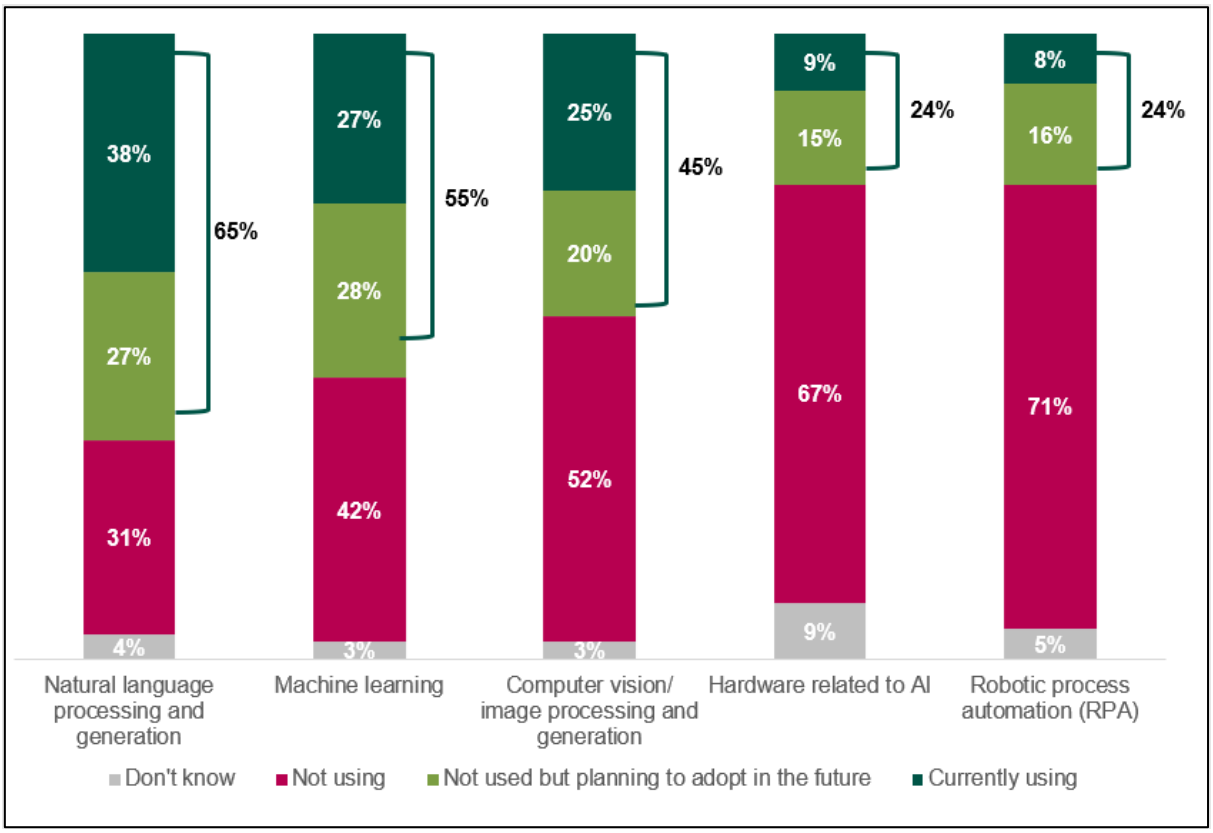
- the types of AI used by organisations;
- how long they have been using them;
- how the AI was adopted; and
- reasons for employing AI technology

Types of AI used

Overall, 68% of businesses were currently using at least one AI technology, while the remaining 32% had plans to adopt AI in the future. Figure 4.1 illustrates the type of AI technologies currently used and planned within these businesses. Natural language processing and generation was most commonly used, with 38% of businesses currently using this type of AI, and a further 27% planning to deploy it in the future. Those in the Information and Communication sector were most likely to be currently using this type of AI (54%).

Businesses in Human Health and Social Work Activities were more likely than businesses overall to be currently using computer vision, image processing and generation (42% compared to 25% overall). Businesses in this sector were also more likely to be currently using hardware related to AI (19% compared to 9% overall). The use of robotic process automation was significantly higher among large businesses (23% compared to 8% overall).

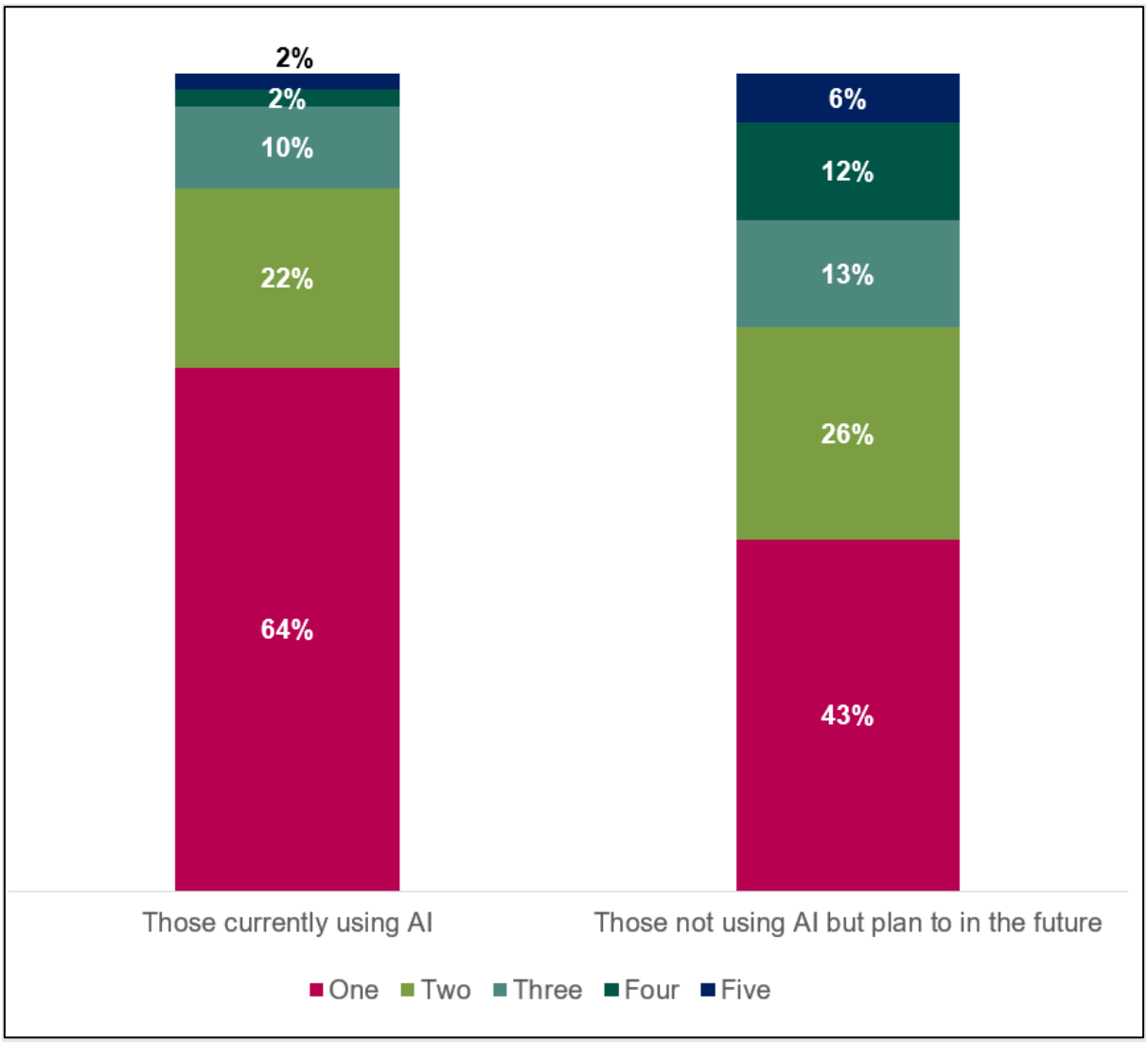
Figure 4.1 Use of AI technologies



B1. For the following Artificial Intelligence technologies, please could you tell me whether your organisation is currently using it (including piloting), not currently but have plans to adopt in the future, or has no plans to use it. Base: All (350)

Of the businesses currently using AI, 64% were deploying one type of AI technology, 22% were using two types of AI, and 14% were using three or more. Meanwhile, among businesses planning to adopt AI in the future, 43% planned to introduce one type of AI, 26% planned to introduce two types of AI and 31% planned to introduce three or more.

Figure 4.2 Number of AI technologies businesses use or plan to use



Count of AI technologies from B1. Base: Those currently using AI (239) and Those not using AI but plan to in the future (111)

Those currently using AI were asked what specific AI products they were using. The most common product was ChatGPT (38%) followed by:

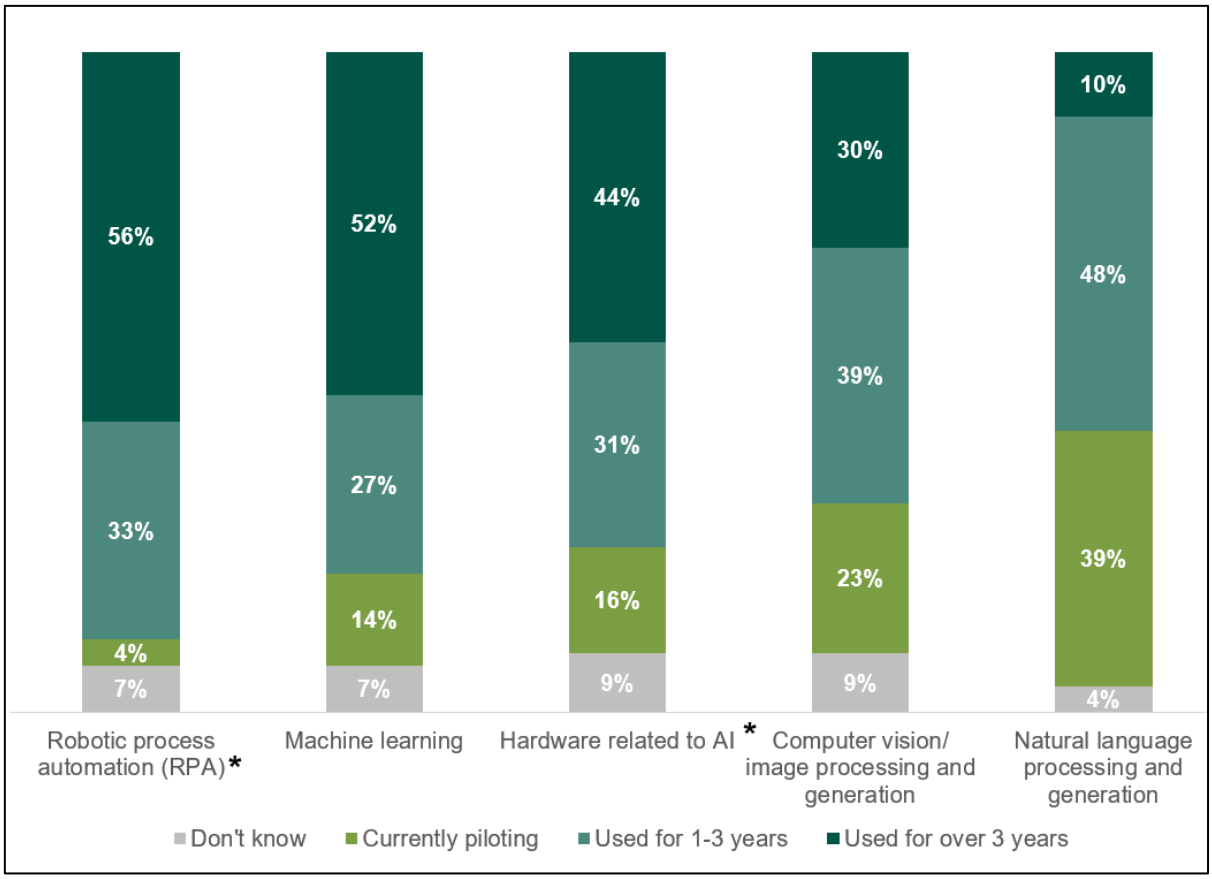
- 15% - AI with hardware and physical products;
- 8% - AI tools within Microsoft office (exc. co-pilot);
- 5% - Microsoft Co-pilot;
- 5% - Gemini (formerly Google Bard);
- 5% - Sage;
- 4% - AI tool within Adobe creative suite; and
- 3% - Xero.

The remaining AI products currently used were mentioned by 2% of businesses or less. Where there were single mentions of products, these remained categorised as “other” in the dataset. 9% of businesses currently deploying AI were unable to name the specific product.

Length of time using AI

For each type of AI technology, over half of businesses have been using it for at least one year. Over half of businesses (52%) using AI within machine learning have been doing so for over 3 years.

Figure 4.3 Length of time using each AI technology

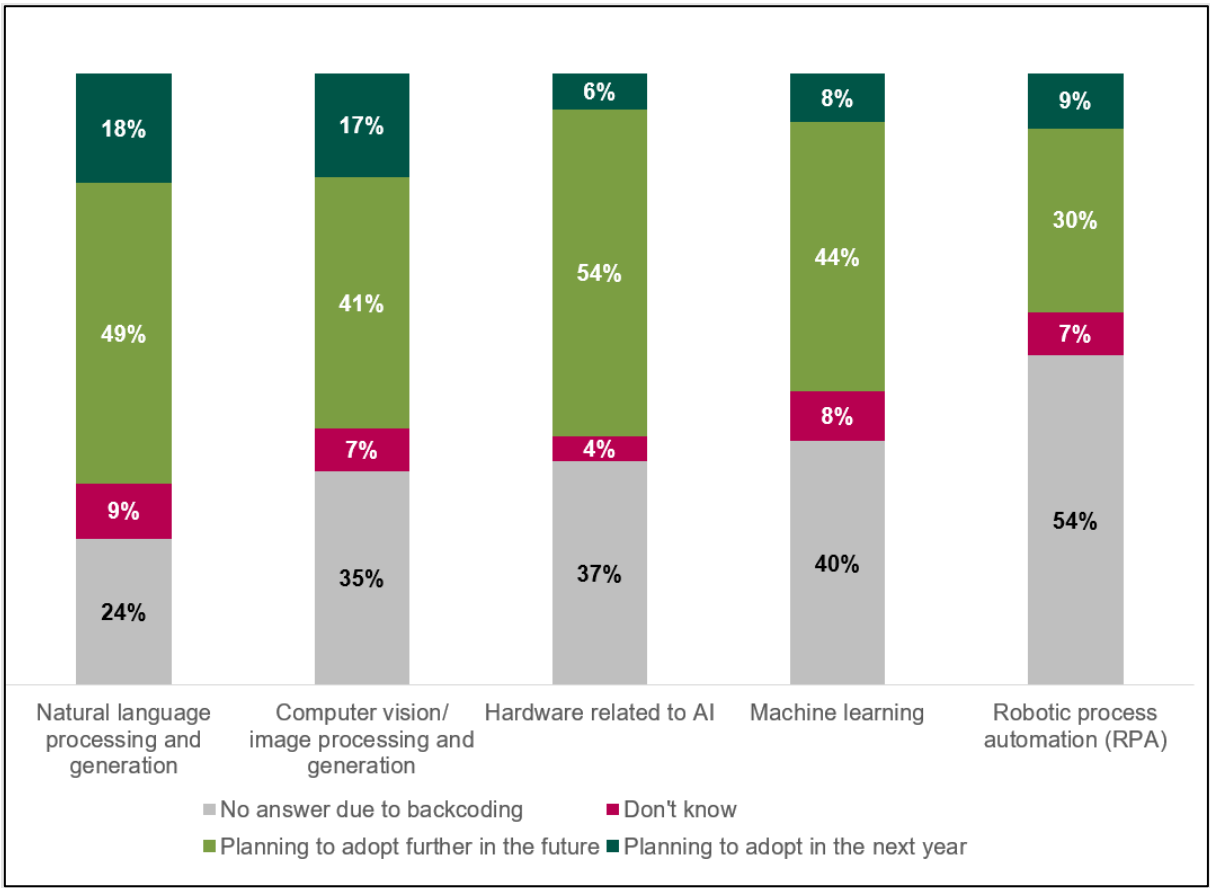


***Caution * denotes low base size**. B2. Please could you tell me whether your organisation is currently piloting the following technology, has used for 1-3 years, or has used for over 3 years. Base: Those currently using AI (239); RPA (27), machine learning (94), Hardware related to AI (32), Computer vision/ image processing and generation (88) and Natural language processing and generation (132)*

Among those who have not yet deployed AI but have plans to do so, they most commonly planned to do this in more than a year’s time. This is true across the different AI technologies, as shown in Figure 4.4. Natural language processing and generation (18%) and computer vision, image processing and generation (17%) were most likely to be adopted in the next year.

A notable number of records were ‘back-coded’ post-fieldwork. This is where respondents initially said they did not use the AI technologies listed but instead used an alternative technology and as such were not asked this question. Post fieldwork, these ‘other’ technologies were reviewed and found to all fall into these five categories of AI and were subsequently back-coded into the appropriate technology.

Figure 4.4 When organisations not currently using AI plan to adopt it



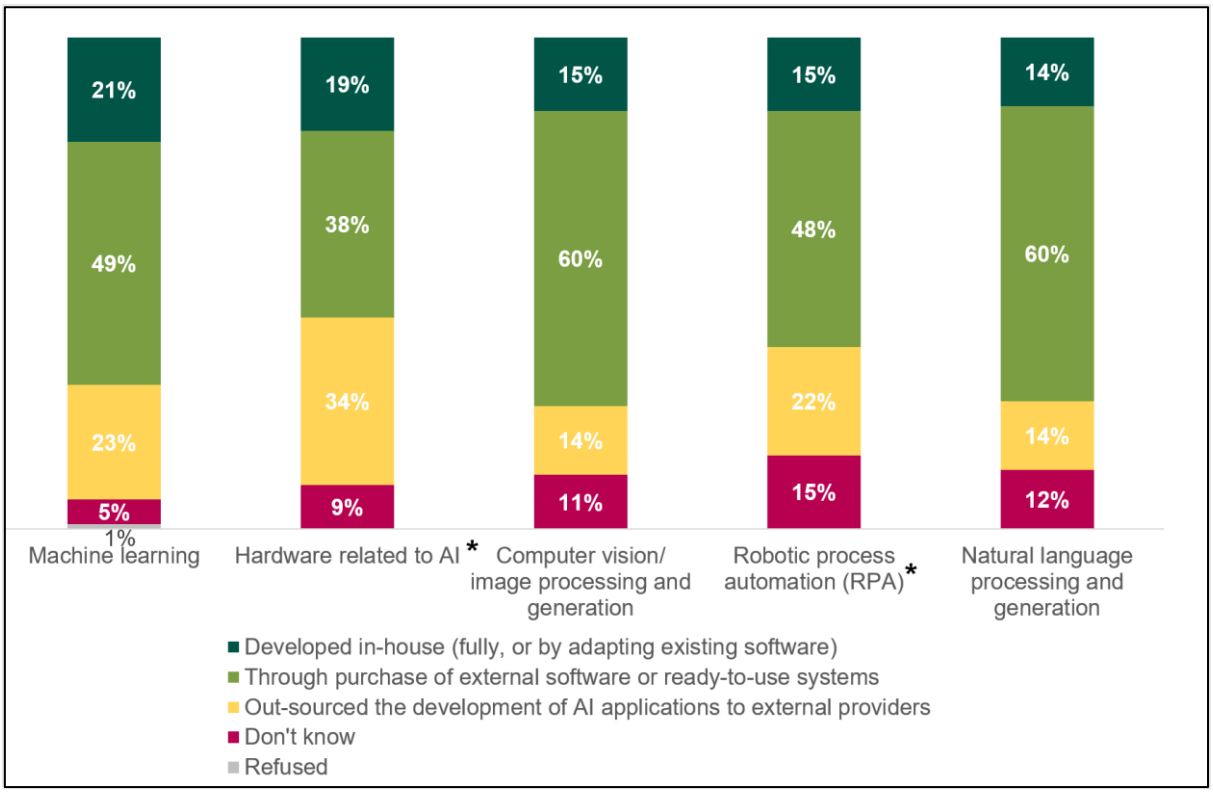
B3. Please could you tell me whether your organisation is planning to adopt the following technology in the next year or whether you plan to adopt it further in the future. Base: Those not using AI but plan to (111); Natural language processing and generation (94), Computer vision/ image processing and generation (69), Hardware related to AI (52), machine learning (98) and RPA (56),

How the AI was adopted

Each AI technology was most commonly adopted through the purchase of external software or ready-to-use systems, shown in 0. Around one in five businesses developed machine learning (21%) and hardware related to AI (19%) in-house. AI development most likely to be outsourced was for hardware related to AI (34%).

Micro businesses were less likely to outsource the development of natural language processing and generation (5% vs 14% among businesses overall) and more likely to purchase external software or ready-to-use systems for computer vision, image processing and generation (78% vs 60% among businesses overall).

Figure 4.5 How the AI technology was adopted

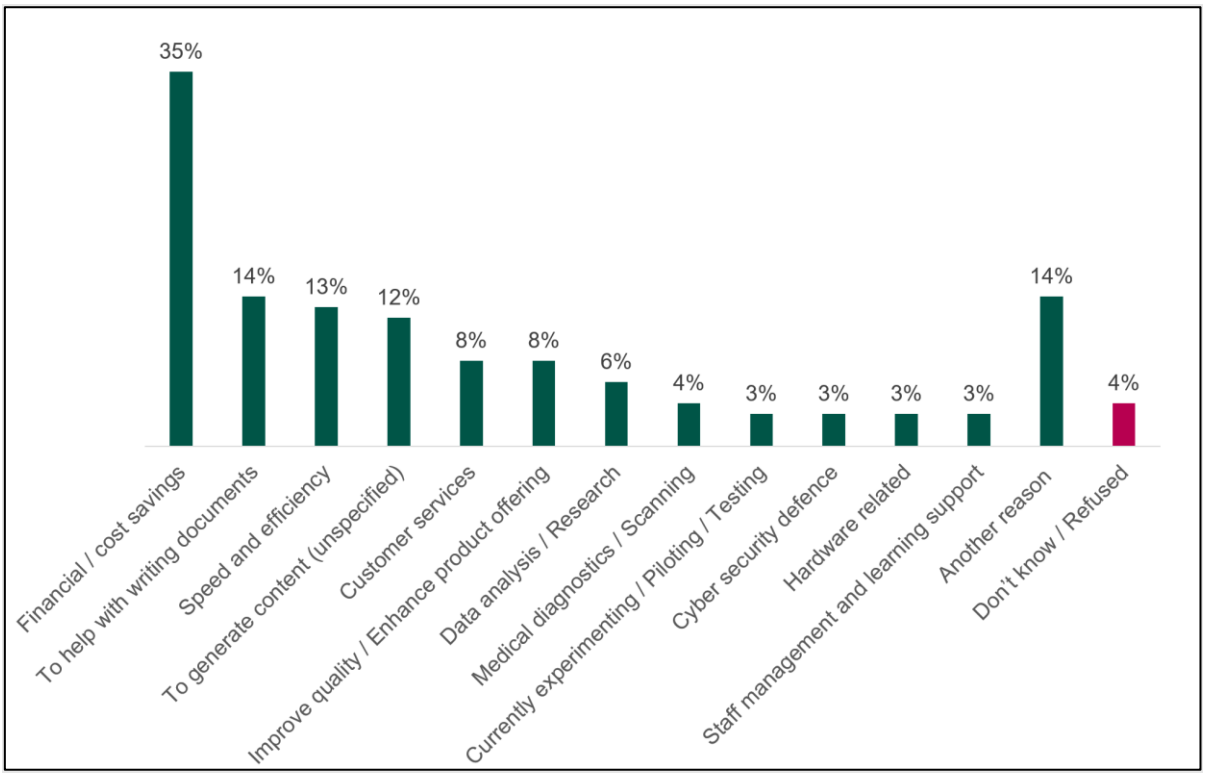


Caution * denotes low base size. *B4. How did your organisation adopt the following technology: [Technology]. Base: Those currently using AI (239); machine learning (94), Hardware related to AI (32), Computer vision/ image processing and generation (88), RPA (27) and Natural language processing and generation (132)*

Reasons for employing AI technology

Just over a third of businesses currently using AI said they did this for the purpose of financial or cost savings to their business (35%). Those that said they had cyber security practices in place explicitly for current AI technologies were more likely to report using AI for financial or cost savings compared to those without such practices in place (42% vs 29%). 14% employed AI to help write documents, 13% cited speed and efficiency purposes, and a further 12% used it for content generation more broadly. 8% reported using AI to improve quality or enhance their product offering.

Figure 4.6 Reasons for employing AI technology



B5. For what reasons does your organisation employ AI technology? Base: Those currently using AI (239)

5 Cyber security practices around AI

This chapter explores organisations' cyber security practices surrounding AI technologies they deploy.

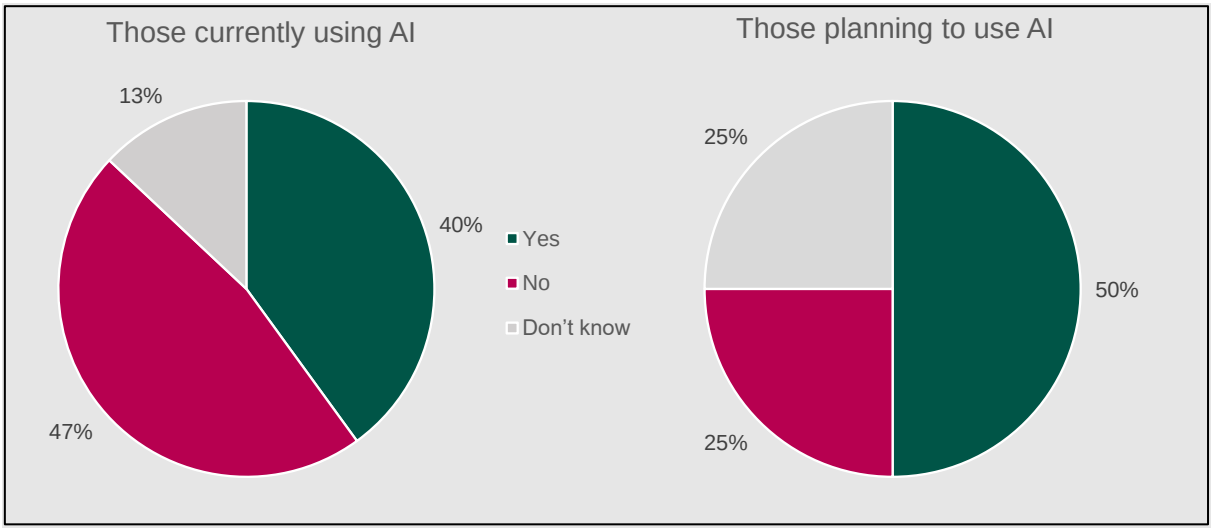
Cyber security practices explicitly regarding AI

Of those currently using AI technologies, as shown in Figure 5.1, two-fifths (40%) said they had specific cyber security practices or processes in place explicitly regarding the AI technology they deploy. Just under one-half (47%) said they did not have such practices in place specifically for AI, and 13% were unsure.

Micro businesses and organisations using only one AI technology were less likely to have cyber security practices in place in relation to the AI technology they deploy (31% and 35% respectively). Similarly, those who had purchased off-the-shelf AI products were less likely to have specific practices in place (31%), while those who had outsourced the development of AI were considerably more likely to have practices in place (63%).[3] Businesses that developed the AI technologies in-house were neither more or less likely to have specific cyber security practices or processes in place compared to businesses overall.

Among those planning to use AI in the future, half (50%) said that their organisation would have specific cyber security practices or processes in place explicitly regarding the AI technology once the planned technologies were deployed. Meanwhile, 25% said that they would not have such practices and 25% were unsure.

Figure 5.1 Whether organisations have, or plan to have, specific cyber security practices in place explicitly regarding AI technology

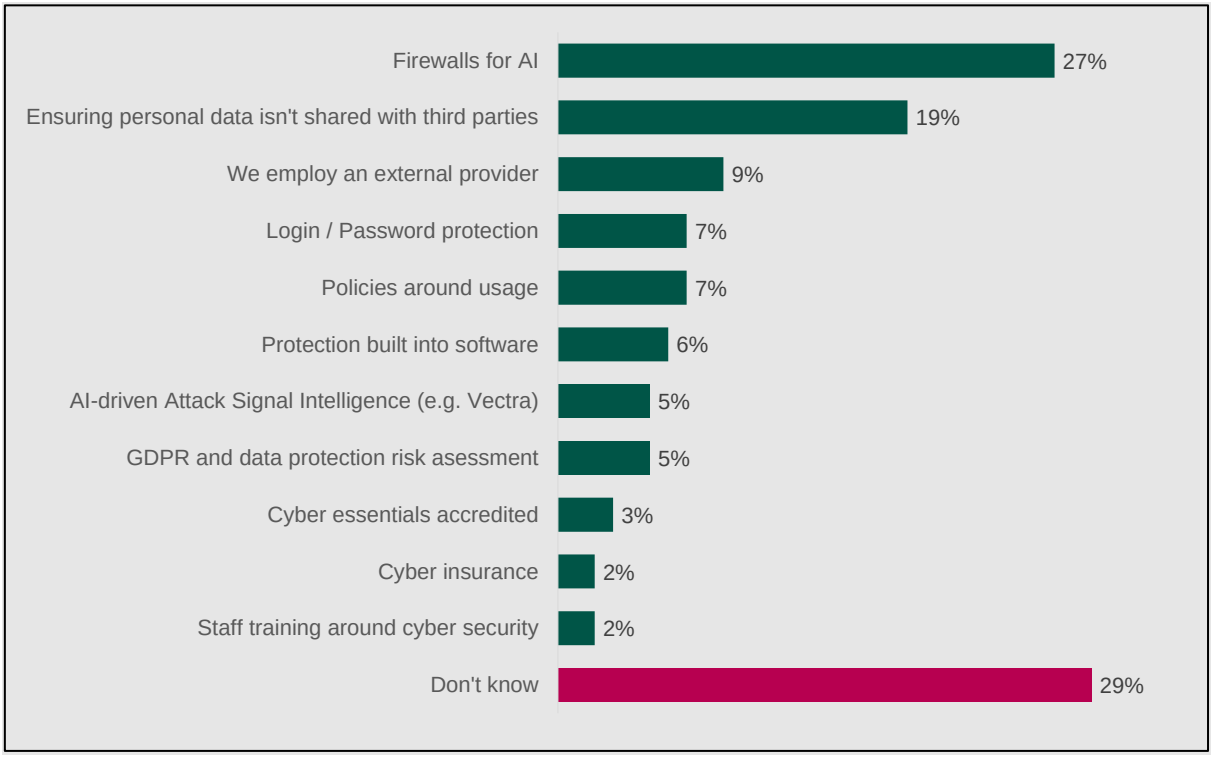


C1. Does your organisation have specific cyber security practices or processes in place explicitly regarding the AI technology you deploy? Base: Those currently using AI technologies (239)
C2. Would your organisation have specific cyber security practices or processes in place explicitly regarding the AI technology once your planned AI technologies are deployed? Base: Those planning on using AI technology (111)

[3] The base size of businesses that outsourced the development of AI is low (35), therefore findings should be treated with caution.

Of those with or intending to have specific AI cyber security practices or processes, just over a quarter mentioned deploying firewalls for AI (27%). One-fifth of organisations reported ensuring personal data is not shared with third parties (19%). As shown in Figure 5.2, just under a third (29%) did not know what exactly these cyber security practices were or would be. Although participants said they were the appropriate person to discuss cyber security, some of those interviewed were not in an IT role and therefore could be why they were unsure of the specific practices and processes in place.

Figure 5.2 Cyber security processes explicitly regarding AI technologies currently deployed or that businesses plan to deploy



C3. Please could you summarise what these practices or processes are/might be? Base: Those with or intending to have specific AI cyber security practices or processes (150)

For those without or not intending to have specific AI cyber security practices or processes, there were a few key reasons as to why they had not adopted specific practices. 14% had not considered it or did not believe they know enough about it, and 14% said they do not use AI for anything sensitive (and therefore deemed it unnecessary). Around one in ten said AI is not widely used enough to warrant specific measures (11%) and that it falls within their general cyber security practices anyway (10%). Those who purchased of off-the-shelf products were more likely to say AI is not widely used enough to warrant specific cyber security measures (18% vs 11% overall).

Two-fifths (39%) of all businesses that took part in the survey said that there were not any specific cyber security requirements or features that they expect to be built into AI companies' models and systems, and a further third (33%) were unsure. One in ten (11%) said that they would expect data protection and privacy to be built in, rising to 23% among large organisations, and 17% among those who purchased off-the-shelf AI tools. Others mentioned higher levels of security (3%), ensuring data sources are legal and reliable (2%) and protection against hacking/cyber-attacks (2%). 3% said security is already built into the AI system. Micro organisations were more likely to say that there were not any specific cyber requirements they would expect to be built into AI companies' models and systems (47% vs 39% overall).

Of those organisations that outsourced the development of their AI technology, 81% said they had not identified a vulnerability or been breached as a result of the AI service deployed in their infrastructure. 11% had identified a vulnerability but not been breached, while 4% had experienced a breach. There was no significant variation across subgroups.

6 General cyber security practices

This final chapter explores general cyber security practices. As stated to organisations that took part in the survey, this means any strategy, processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.

General cyber security practices

When asked more generally about cyber security practices, 90% of all businesses had at least one governance or risk management arrangement in place. Just under three-quarters (72%) had a formal policy or policies in place covering cyber security risks, and around two-thirds had either a Business Continuity Plan that covers cyber security (67%), or a written list of the most critical data, systems or assets that their organisation wants to protect (64%).

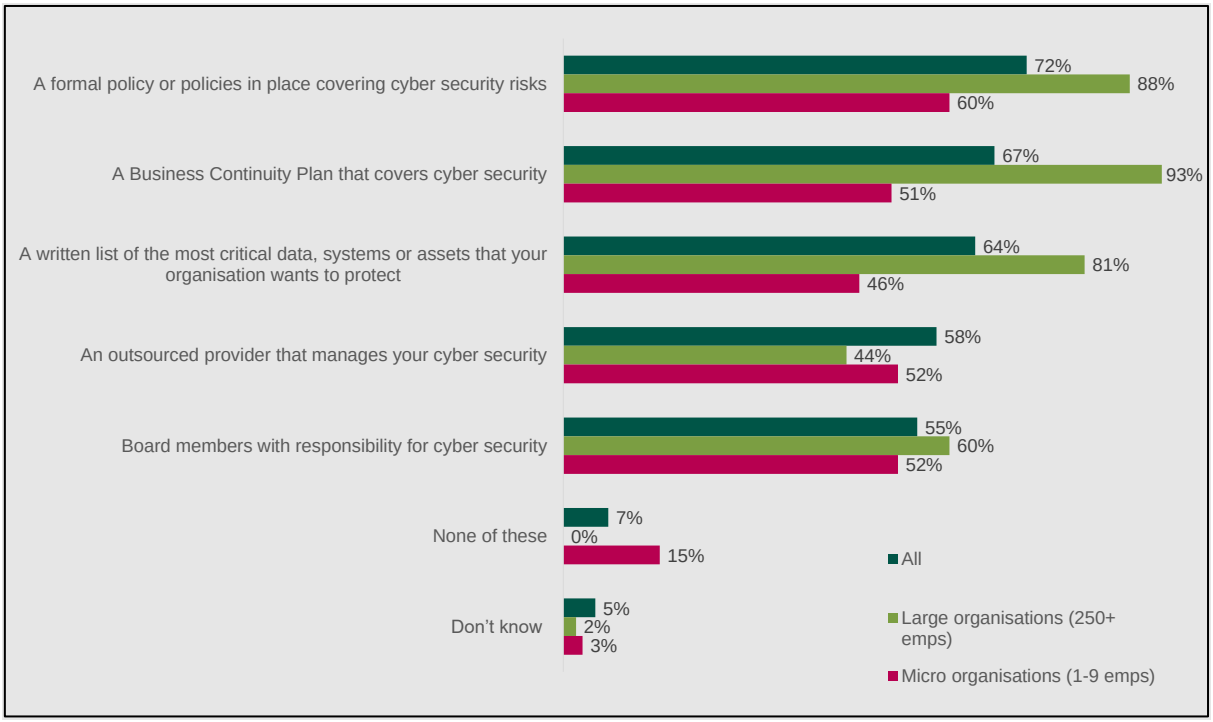
As shown Figure 6.1, findings varied considerably by the size of the organisation. Large businesses were more likely to have all three of these arrangements in place (88%, 93% and 81% respectively). Micro businesses on the other hand tended to be less likely to have one of these arrangements in place, with 15% stating that they had none of them at all. 7% of all businesses had none of the risk management arrangements listed, and 3% said they were unsure.

There were also some differences by sector. A formal policy or policies in place covering cyber security risks was most common among those in Human Health and Social Work Activities (85%). A Business Continuity Plan that covers cyber security was most common among those in Financial and Insurance Activities (85%). An outsourced provider that manages their cyber security was most prevalent in the sector group consisting of Electricity, Gas and Air Conditioning Supply; Water Supply; Sewerage, Waste Management and Remediation Activities; and Transportation and Storage (72%), as well as those in Financial and Insurance Activities (72%). Organisations in the Information and Communication sector and Financial and Insurance Activities were most likely to have board members with responsibility for cyber security (69% and 72% respectively).

Those with cyber security practices in place explicitly for AI technologies were more likely to have:

- An outsourced provider that manages their cyber security (67% vs 58% overall);
- A formal policy or policies in place covering cyber security risks (87% vs 72% overall);
- A Business Continuity Plan that covers cyber security (83% vs 67% overall); and
- A written list of the most critical data, systems or assets that their organisation wants to protect (75% vs 64% overall).

Figure 6.1 Governance or risk management arrangements currently in place

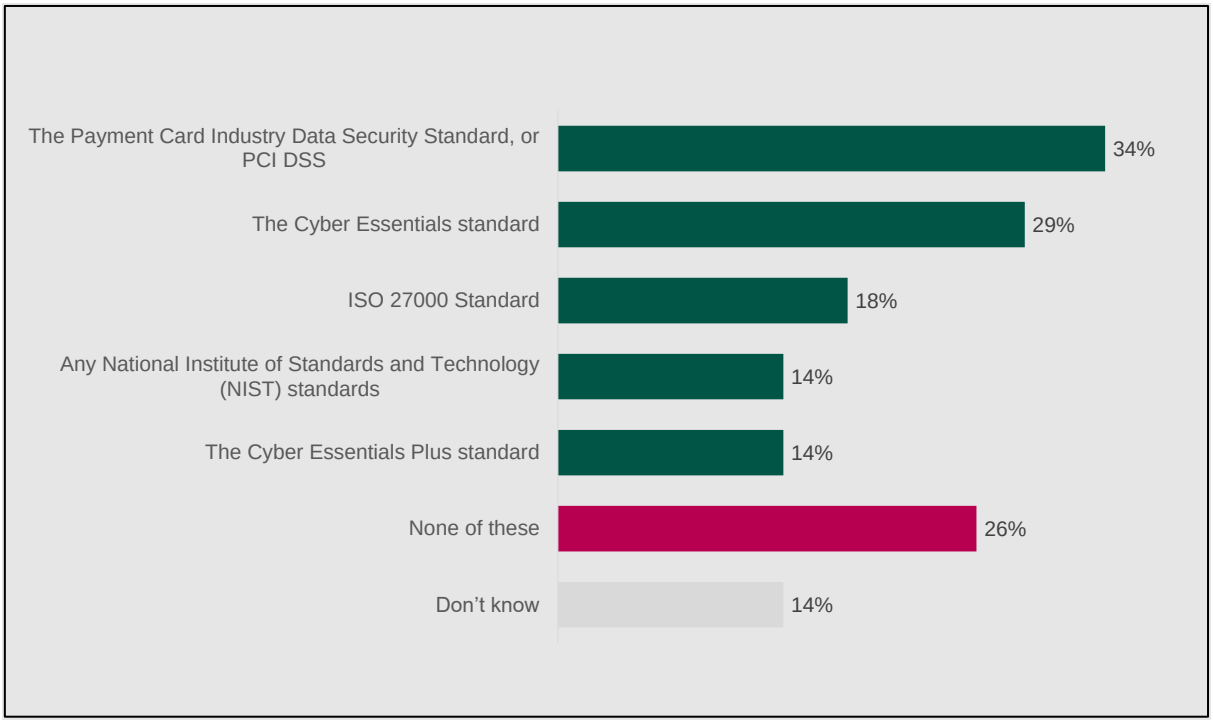


D1. Which of the following governance or risk management arrangements, if any, do you have in place? Base: All (350)

When asked about specific cyber security standards or accreditations, as shown in Figure 6.2, 34% of organisations said they adhered to the Payment Card Industry Data Security Standard (PCI DSS). This compares to 27% of businesses in the Cyber Security Breaches Survey 2023.[4] Around three in ten (29%) adhered to the Cyber Essentials standard, and a further 12% followed the Cyber Essentials Plus standard (compared to 5% and 2% respectively in the Cyber Security Breaches Survey). Just under one-fifth (18%) conformed to the ISO 27000 Standard (compared to 9% of businesses that adhered to the ISO 27001 in the Cyber Security Breaches Survey), and 14% followed any National Institute of Standards and Technology (NIST) standards (compared to 3% of businesses that adhered to the ISO 27001 in the Cyber Security Breaches Survey). Around one-quarter of organisations were not adhering to any of these standards (26%), and 14% were unaware.

[4] Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

Figure 6.2 Standards or accreditations adhered to by organisations



D2. Which of the following standards or accreditations, if any, does your organisation adhere to? Base: All (350)

The Cyber Essentials standard was more likely to be adhered to by large and medium-sized businesses (49% and 44% respectively), and those in the Information and Communication sector (46%).

The Cyber Essentials Plus standard was more likely to be adhered to by medium-sized businesses and those in the Information and Communication sector (25% and 23% respectively).

Any National Institute of Standards and Technology (NIST) standards were more likely to be adhered to by large businesses (33%).

The Payment Card Industry Data Security Standard was more likely to be adhered to by those in the Wholesale and Retail sector (49%) and the ISO 27000 Standard was more likely to be adhered to by those in the Information and Communication sector (31%).

Meanwhile, micro businesses and those in the Professional, Scientific and Technical Activities sector were more likely to not adhere to any of these standards (40% and 42% respectively).

Over the last 12 months, just over three-quarters (78%) of businesses had taken at least one of the measures listed in Figure 6.3 in an effort to identify cyber security risk. This compares to 51% of businesses that had taken at least one measure in the Cyber Security Breaches Survey 2023. [5] The most common measures taken by organisations were to conduct a risk assessment covering cyber security risk (59%, compared to 29% of businesses in the Cyber Security Breaches Survey), or to invest in specific tools designed for security monitoring, such as Intrusion Detection Systems (55%, compared to 30% of businesses in the Cyber Security Breaches Survey). Those in the Financial and Insurance Activities sector were most likely to have conducted a risk assessment covering cyber

[5] Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

security risks (74%) and those in the Information and Communication sector were most likely to have used specific tools designed for security monitoring (75%).

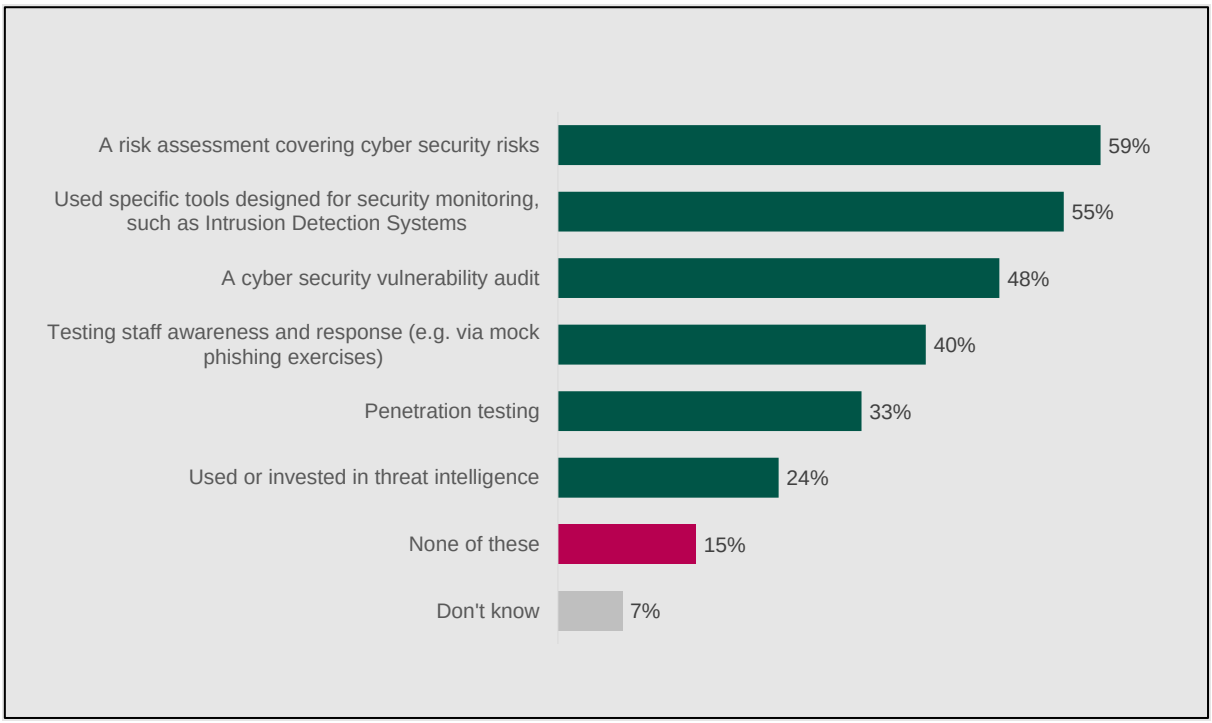
Just under half (48%) had conducted a cyber security vulnerability audit (compared to 15% of businesses in the Cyber Security Breaches Survey), rising to 65% of businesses in the Information and Communication sector, and 64% of those in the Financial and Insurance Activities sector.

Two-fifths (40%) had tested staff awareness, for example via mock phishing exercises. This compares to 19% of businesses in the Cyber Security Breaches Survey. A third of businesses (33%) had carried out penetration testing, compared to 11% of businesses in the Cyber Security Breaches Survey. Around a quarter of businesses (24%) had used or invested in threat intelligence, compared to 9% of businesses in the Cyber Security Breaches Survey.

Large businesses were more likely to have taken any of the measures listed in Figure 6.3 than the average across businesses of less than 250 employees.

15% of businesses had taken none of the measures listed in the survey to identify cyber security risks to their organisation, rising to one-quarter (25%) among micro businesses. 7% were unaware if their organisation had undertaken any of these activities.

Figure 6.3 Actions taken to identify cyber security risks over the last 12 months



D3. Which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation? Base: All (350)

7 Appendix: Glossary

Artificial Intelligence (AI): The broader field encompassing knowledge-based systems, data-driven and machine learning-enabled systems, including classic machine learning (supervised learning, unsupervised learning), deep learning, and reinforcement learning, referring to the development of systems that can perform tasks requiring human intelligence.

Machine learning: Encompasses algorithms that can acquire knowledge from data and generate classification, predictions, or pattern without explicit programming, facilitated by labelled data (supervised learning) or unlabelled data (unsupervised learning).

Computer vision/ image processing and generation: The use of artificial intelligence programming to produce, generate, analyse, interpret, and manipulate digital images.

Hardware related to AI: Examples include Edge Computing Chips, Quantum Hardware, Application Specific Integrated Circuits (ASIC), Neuromorphic Hardware, and Field Programmable Gate Array (FPGA).

Natural language processing and generation: The use of artificial intelligence programming to produce written or spoken narratives from a data set, including creating computer code or transcribing audio to text in real time.

Robotic Process Automation (RPA): A software technology that makes it easy to build, deploy, and manage software robots that emulate humans actions interacting with digital systems and software.

“

IFF Research illuminates the world for organisations businesses and individuals helping them to make better-informed decisions.”

Our Values:

1. Being human first:

Whether employer or employee, client or collaborator, we are all humans first and foremost. Recognising this essential humanity is central to how we conduct our business, and how we lead our lives. We respect and accommodate each individual’s way of thinking, working and communicating, mindful of the fact that each has their own story and means of telling it.

2. Impartiality and independence:

IFF is a research-led organisation which believes in letting the evidence do the talking. We don’t undertake projects with a preconception of what “the answer” is, and we don’t hide from the truths that research reveals. We are independent, in the research we conduct, of political flavour or dogma. We are open-minded, imaginative and intellectually rigorous.

3. Making a difference:

At IFF, we want to make a difference to the clients we work with, and we work with clients who share our ambition for positive change. We expect all IFF staff to take personal responsibility for everything they do at work, which should always be the best they can deliver.

IFF Research

5th Floor
St. Magnus House
3 Lower Thames Street
London
EC3R 6HD
Tel: +44(0)20 7250 3035
Website: iffresearch.com

Contact details: