March 2024

MARKET REPORT

SMB cyber resilience in Japan

Navigating through doubt to an AI-powered future

Barracuda®
Your journey, secured.

Table of Contents

Executive summary

The release of the generative artificial intelligence (AI) tool ChatGPT in November 2022 changed the global perception of AI. Seemingly overnight, AI became a mainstream field of computer science. Today, the challenge facing every organization and national government is how to understand and address the risks and uncertainties that are being introduced or accelerated by AI, while at the same time harnessing its potential for good.

To better understand how smaller organizations in Japan are coping with this challenge, we commissioned research that explored the varied perceptions, concerns, and applications of AI among businesses in Japan with fewer than 200 employees. The findings show that while respondents are largely positive and optimistic about AI, there is considerable doubt and concern about how AI impacts the business and the cyberthreat landscape and whether they have the skills to cope.

The main findings include:

- 66% expect AI to reduce headcount.
- 76% expect AI to make it easier and quicker to gather customer insight.
- 77% need partners to help them implement and manage AI solutions.
- 62% say any business use of generative AI is unofficial — 69% worry about the risks.
- 55% are unsure how attackers might leverage AI in email-based attacks — although 36% believe AI will strengthen protection against such threats.
- 63% lack some or all the skills they need to cope with AI-based cyberattacks.

This report summarizes the research findings, their context, and the implications for organizational cyber resilience in the age of AI. We hope they will help companies to benchmark their own AI maturity and identify areas for action and support.

Research methodology

Barracuda commissioned independent market research firm Tech Research Asia to survey 500 IT professionals in organizations of between 50 and 200 employees in Japan, with a balanced representation of company sizes and industry sectors. Just under half (47%) of respondents held a C-suite role. The survey was fielded in November 2023.

Introduction

Artificial intelligence and its impact on the world

Artificial intelligence (AI) is a field of computer science that can perform complex or time-consuming tasks that in the past could only be done by humans, such as such as reasoning, learning, perception, natural language processing, problem-solving, and decision-making.

AI combines computer science and robust, often vast, datasets. AI has many subfields, such as generative AI (GenAI), machine learning, neural networks, natural language processing, computer vision, cognitive computing, and deep learning. Each subfield has its own goals, methods, and applications.

The development and implementation of AI is evolving rapidly. The potential rewards for businesses and society are significant, but there are also some associated risks.

For example, AI can boost business performance and competitiveness by optimizing and automating processes, reducing costs, increasing quality, and generating new insights and ideas. It can enhance customer service and interaction through chatbots and turn customer data into deep insight. It can also help businesses tackle challenging, complex, and novel problems that require high levels of intelligence — such as cybersecurity.

However, AI systems can also be time-consuming and costly to develop and implement, and they often require specialist skills and resources that can be hard to recruit. AI is likely to reduce the need for some jobs roles, which has long-term social implications. In addition, there are privacy and data protection concerns associated with the use and storage of vast volumes of personal, sensitive, and confidential data — and ethical and legal issues such as accountability and transparency.

When it comes to cybersecurity, the AI tools that can enhance threat prevention, detection, and response can also be used by cyberattackers to launch ever more sophisticated and targeted attacks, faster.

The AI landscape in Japan

The challenge facing every organization and national government, including in Japan, is how to address the risks and uncertainties of the rapidly evolving field of AI, while accelerating beneficial innovation and adoption.

Japan has a longstanding reputation of being risk-averse, but also for innovation, and in the field of AI Japan is a leader in smart robotics and automotive technologies. According to some reports, however, Japan's strength in AI-powered hardware is not matched by equal success in AI-based software. Japan remains relatively dependent on foreign large language models for generative AI, for example. Japan faces some other unique challenges in the development and adoption of AI, including a lack of data availability, and cultural factors around acceptable levels of business risk.

However, the Japanese authorities are keen to implement AI-related regulations that are risk-based, agile, and collaborative and that enable society and businesses to reap the full rewards of artificial intelligence as part of the journey towards "Society 5.0."

FINDING #1

AI will reduce SMB headcount, add insight — but help is needed to realize benefits

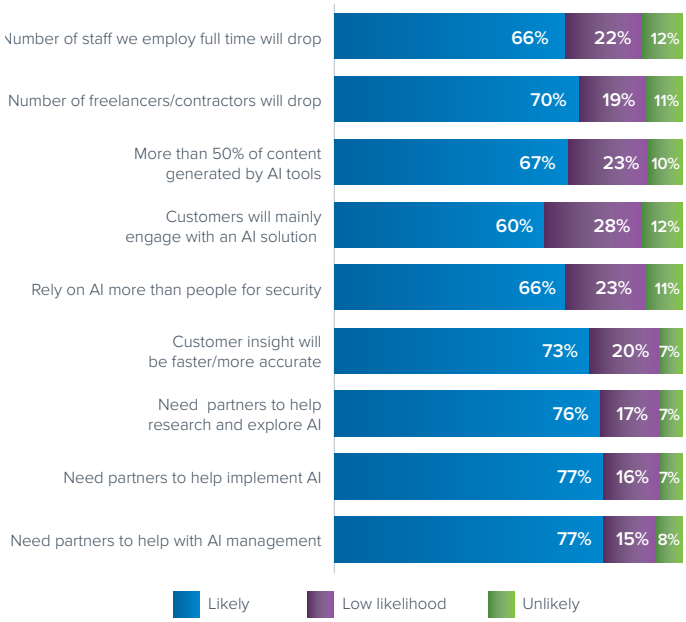
The research findings suggests that many smaller organizations in Japan feel optimistic about the business impact of AI.

Most expect that over the next two years, the use of AI solutions will lead to a reduction in headcount, both in terms of full-time employees (66% of respondents) and freelancers or contractors (70%). This is likely to reduce costs and the human resource burden for the employer, but it also points to an uncertain future for employees whose role might be under threat.

AI is also expected to enhance operational efficiency, including in areas such as marketing and customer relationship management. 67% expect more than half of their content to be generated by AI tools within the next two years, while 60% believe that customers will primarily engage with an AI solution (for example a chatbot) as the main communications channel. Alongside this, 76% expect that customer insight will be more accurate and quicker to collect.

At a general, rather than threat-specific level, 65% believe that an ability to rely on AI tools for security will reduce the need to employ additional security staff or engage a third party. AI has a significant role to play in cybersecurity, particularly in the automated detection, analysis, and response to threats — tasks that are traditionally manual, time- and resource-intensive, and prone to false positives. Because Japan faces one of the world's most acute cybersecurity shortages — see page 7 below — using AI to help organizations of all sizes to make the most of their security resources is critical for protection.

Beyond security, how will AI impact your organization in the next 2 years?



Base: all research participants, n=500

The power of partnerships

Most organizations believe they need help to achieve the full business benefits of AI.

Three-quarters of the businesses surveyed said they needed partners to help them research and explore the field of AI (76% of respondents), to help them implement or build AI solutions (77%), and to help with ongoing services to manage AI solutions (77%).

Security vendors, managed service providers, and others in Japan have a great opportunity to support smaller businesses in harnessing and reaping the rewards of AI.

FINDING #2

62% say any business use of generative AI is unofficial — many worry about risks

In November 2022, a free research preview of a generative AI tool, ChatGPT, was released by OpenAI. ChatGPT is a chatbot that uses large language models to generate natural and engaging conversations based on user prompts. The functionality and speed of ChatGPT and other generative AI tools, such as Bing, took the world by storm.

Behind the headlines, however, there is less certainty and more concern when it comes to generative AI and the use of such tools in the workplace.

An awareness of GenAI is also not the same as a broad understanding of the field of artificial intelligence. While 56% of respondents claimed to understand the difference between generative AI and other forms of AI, such as machine learning — 44% admitted that they either didn't know or were only somewhat sure.

The findings show that businesses in Japan understand the potential rewards of AI, but they are also aware of the associated risks. And this means that there are often restrictions placed on its use.

Risks and restrictions for generative AI

69% of respondents believe there are risks associated with the use of generative AI in the workplace.

Despite this, 18% of respondents overall said they allow generative AI to be used in the workplace — 6% say it is used extensively, and 12% sanction its use only by specific teams or individuals.

A further 62% say it is not used "officially," which suggests that many businesses are aware that employees could be using generative AI but in ways that are unmonitored and unmanaged, increasing the potential security risks.

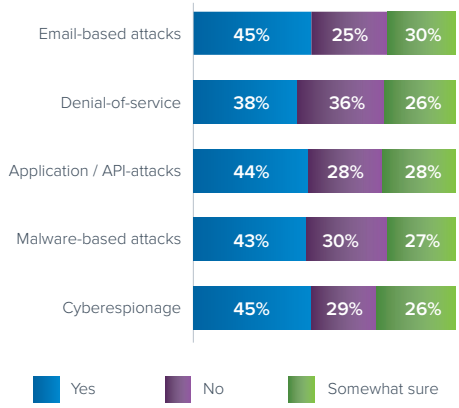
Other areas of concern related to generative AI are data protection and privacy concerns based on the large volume of information stored and analyzed (57% of respondents), the lack of a regulatory framework for AI implementation (47%), and a lack of insight into how the AI systems make decisions (31%). 13% worry that cyberattackers may compromise their AI systems to weaponize their defenses against them.

FINDING #3

More than half are unsure how attackers might leverage AI in common cyberthreats

Businesses are uncertain about how AI will transform common cyberthreats. For example, 55% of respondents say they don't know or are unsure of how attackers might use AI in email-based attacks. A similar proportion felt this way about denial-of-service attacks (62%), malware-based attacks (57%), application/API attacks (56%), and cyber espionage (55%).

Do you know how AI might be used in the following attack types?



Base: all research participants, n=500

FINDING #4

Email threats the top security concern — but 36% believe AI will strengthen protection

These findings are worrying because email-based threats top the list of security concerns for smaller businesses in Japan. 53% of respondents listed account takeover attacks as one of their top three concerns.

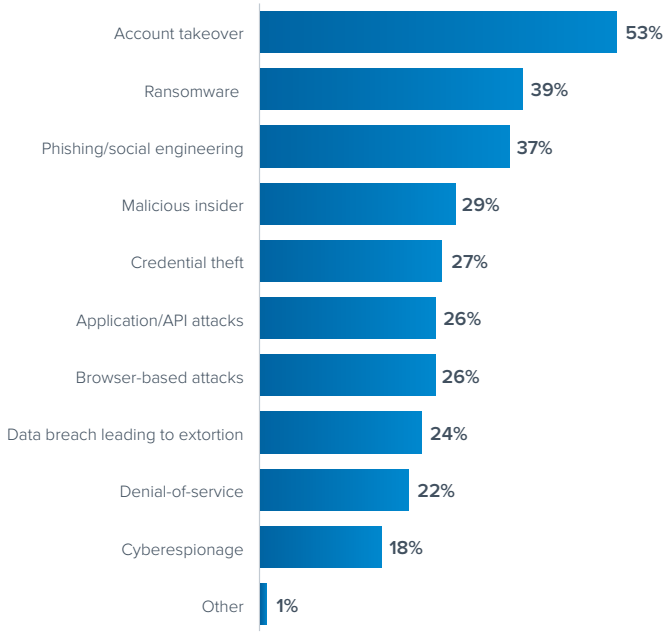
Account takeover is an advanced email threat. It is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials. By posing as the real user the attacker can then change account details, send out phishing emails, steal financial information or sensitive data, or use any stolen information to access further accounts within the organization.

Other email-based threats, such as phishing and social engineering in general, made the top three concerns for 37% of respondents.

The anxiety around email-based attacks is not surprising because they are often the starting point for other, more severe incidents, including ransomware, data breaches, cyber espionage, and more. For example, 39% of respondents listed the threat of ransomware among their top three concerns, and our research shows that in 2022 69% of successful ransomware attacks started with an email.

For more information on email-based security threats, check out Barracuda's guide to the 13 email threat types.

Which of the following cyber threats do you worry about the most?



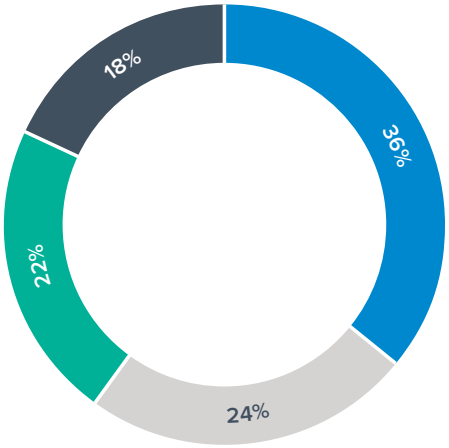
Base: all research participants, n=500

The role of AI in strengthening defenses

The role of AI in strengthening cyber defenses is relatively well understood by survey respondents, particularly when it comes to email security and cybersecurity awareness training for employees. There is some uncertainty about how AI can help in other areas, but this could be due to those areas themselves being less well understood by smaller businesses.

When asked to choose which AI-strengthened cyber defenses would make the most difference to their organizational security, 36% chose AI-boosted email security, particularly for defending against advanced AI-based threats such as deepfakes. 24% said AI would enable more frequent, personalized training. The role of AI in threat intelligence and 24/7 threat detection and response, such as that conducted by security operations centers (SOCs) was less well understood.

Which of the following AI applications in strengthening cyber defenses do you think will make the most difference to your organizational security?



- AI will enable security technologies to identify and respond to advanced email threats, such as deepfakes, much faster, automatically, and at scale.
- AI can help to educate users more frequently with personalized training content.
- AI will enable defenders to share and use threat intelligence updates with other organizations/customers in real time.
- AI will enhance the work of 24/7 human threat analysts by putting security alerts in context and advising on remedial action, based on a deep, learned understanding of previous decision-making processes and outcomes.

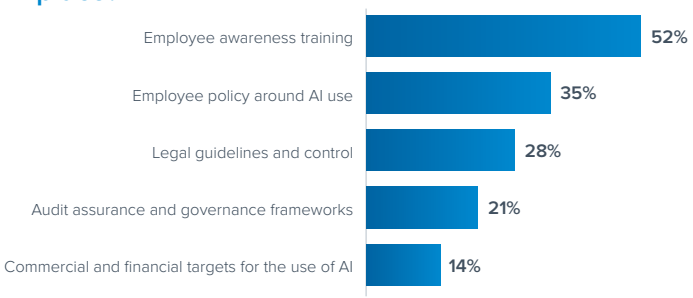
Base: all research participants, n=500

FINDING #5

Few businesses are ready for AI-based threats — lack skills, policies

Overall, survey respondents lack the AI-specific practices and policies they need to ensure AI is used responsibly. While a relatively reassuring 52% run employee awareness training on the use and vulnerability of AI, only 35% have company policies in place regarding what employees can and cannot do with AI. Even fewer have governance guardrails, including legal guidelines, frameworks, and more. This suggests that the business application of AI is often uncontrolled and unmanaged.

If you use AI, which of the following do you have in place?



Base: all research participants, n=500

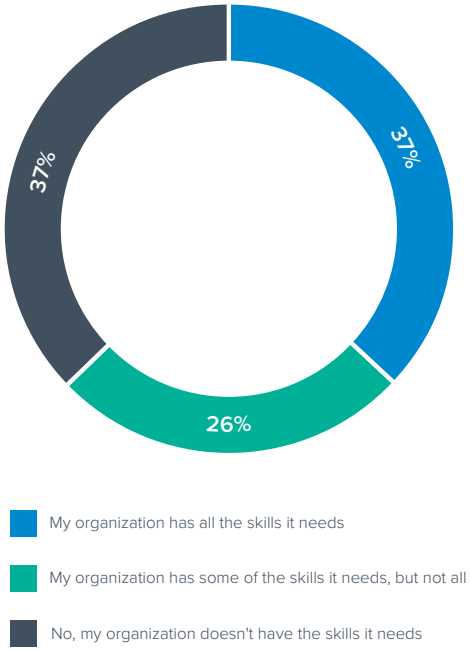
The cybersecurity skills shortage

According to the latest ICS2 Cybersecurity Workforce Study, Japan has a cybersecurity workforce of just under half a million professionals (480,659). This represents a remarkable year-on-year increase of 23.8%, compared to a global increase of 8.7%.

However, demand is significantly outstripping supply. The gap between the number of cybersecurity professionals that Japan has, compared to what it needs is 110,254 people. This is an increase of 97.6% year-on-year, compared to a global rise of 12.6%. No other country assessed by ICS2 has a gap anywhere near this big.

It is interesting to see how this high-level picture is reflected in the daily reality for the smaller businesses surveyed — and for AI-based cyberattacks in particular.

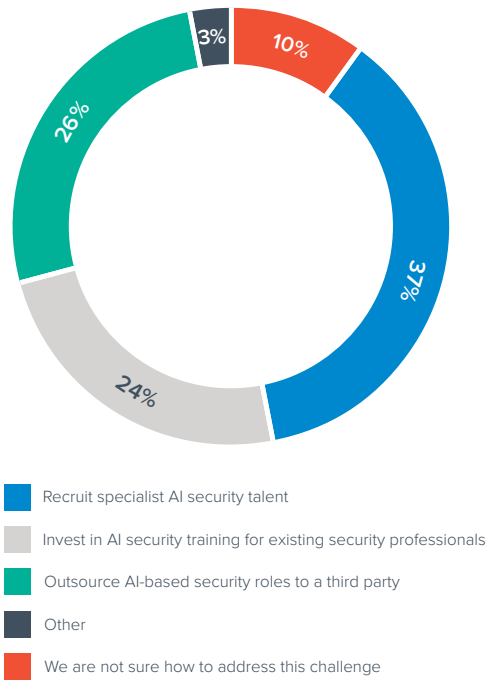
Do you feel your organization has all the skills it needs to cope with AI-based cyberattacks?



Base: all research participants, n=500

The data shows that just 37% of respondents feel they have all the skills they need to cope with AI-based cyberthreats, while 63% say they lack some or all the skills required.

How do you plan to address the AI security skills gap?



Base: all research participants, n=500

When it comes to addressing the skills challenge, the numbers don't really add up.

37% expect to recruit externally the specialist AI security expertise the business needs, with 26% looking to outsource their AI security roles to a third party. They are likely to all be competing for the same limited pool of AI-skilled security professionals.

24% are planning to develop the skills themselves by investing in AI security training. These newly trained professionals may well find themselves a target for roles in third-party organizations and other companies keen to recruit their newly acquired skills. Larger companies able to offer bigger salaries and career progression may find it easier to attract the best talent.

One in 10 has no idea how they are going to address the AI security skills gap.

The good news is that the Japanese security industry understands the scale of the challenge. A number of Japanese universities, including the universities of Tokyo, Kyoto, and the Tokyo Institute of Technology rank among the top 100 universities in the world for AI, and there are programs for professional certification and international collaboration to address the capability gap.

Conclusion

Boosting cyber resilience in the age of AI

To boost cyber resilience in the age of AI, organizations need to shift their security mindset from “preventative” to “detection and response.” This means deploying tools that can capture the signals of a cyberattack in its early stages (on the left-hand side of the MITRE ATT&CK ‘cyber kill chain).

The early stages of the cyber kill chain include reconnaissance, such as scanning for weak access points and unpatched vulnerabilities, collecting the assets the attackers need to mount an attack, such as user credentials captured through phishing, and initial access to a target network, for example through phishing, supply chain compromise, and more.

A good place to start is by embracing generative AI-enabled security tools to counter attackers who are already deploying generative AI to build their cyber weapons, such as increasingly convincing phishing emails.

These AI-enabled security tools can allow IT security professionals to use natural language to gather intelligence when early signals of an attack are detected. The team will quickly get data they can trust and use. This will speed up the response and prevent further damage. It’s like developing immunity instead of just blocking and tackling threats as you would with a purely preventative mindset.

Generative AI can also help organizations to provide employees with perspective and context in security awareness training. In the age of AI, when threats will evolve at speed, regular awareness training on the latest threats and trends will be more essential than ever.

In addition, organizations need to start paying attention to their software-as-a-service (SaaS) applications. These are the new entry routes for attackers armed with stolen credentials. Having the right tools to discover, manage, and secure SaaS applications will also help organizations stay closer to the left of the MITRE ATT&CK framework — which is where they need to be when the AI-powered threats come calling.

Sources of further information and advice

- The 13 email threat types
- Ransomware in the age of AI

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

About Tech Research Asia

Tech Research Asia (TRA) is a technology research, consulting and advisory firm working across Asia Pacific specialising in analysing trends in technology and the impact on business value.

For more information, visit www.techresearchasia.com

Barracuda®
Your journey, secured.