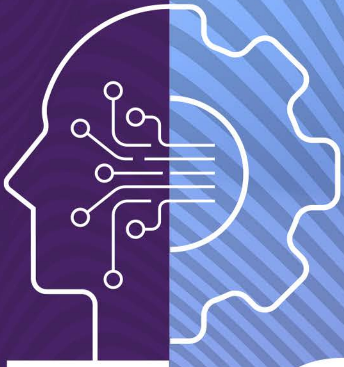
CARBONITE® + WEBROOT®
opentext™ Business Solutions



FACT OR FICTION

Perceptions and Misconceptions on AI and Machine Learning in Cybersecurity

Perspectives from enterprises, businesses, and consumers worldwide

EXECUTIVE SUMMARY

Stop. Think.

What do the terms artificial intelligence and machine learning mean to you? If what comes to mind initially is a vague notion about science fiction concepts, you're not alone. Even IT pros at large enterprise organizations with over 1,000 employees can't escape pop culture visions fed by films and TV. But let's add further context. What do these terms mean to you when you think about the role they might play in cybersecurity?

Historically, we've seen significant global confusion around artificial intelligence (AI) and machine learning (ML) technologies and their role in cybersecurity and business continuity. And yet, adoption continues rising. In our latest survey, featured in this report, the majority of enterprises (93%) use AI/ML, yet 55% admit they are unsure what that means. According to our year-over-year figures, even though the level of understanding around these tools is increasing, that increase is happening at a significantly slower pace than the adoption rate.

Today, as cyberattacks abound and businesses and individuals continue to navigate the remote work culture brought on by the COVID-19 pandemic, maintaining uptime and continuity has never been more critical. Without technologies like AI and ML, which can automatically and drastically improve threat detection, protection, and prevention, the threats to business continuity and overall resilience grow exponentially.

For the purposes of this report, we surveyed IT decision-makers at enterprises (1000+ employees), small and medium-sized businesses (<250 employees), and consumers (home users) throughout the U.S., U.K., Japan, and Australia/New Zealand to gain a deeper understanding of their stance on AI/ML, cybersecurity at large, and how they perceive AI/ML cybersecurity vendors and other businesses in terms of their own security capabilities. The results clearly demonstrate the necessity for increased awareness and transparency about these tools and their role in continuity and security. By improving understanding, businesses can better position themselves to attract and retain customers, and both businesses and individuals the world over benefit from greater resilience against modern attacks.

TABLE OF CONTENTS

ENTERPRISES

1000+ EMPLOYEES

United States

- Most likely to look for AI/ML cybersecurity vendors that use the most technologically advanced methods to combat cyber threats vs. those with the most experience in combating cyber threats
- Experience the most challenges with integration when implementing a cybersecurity solution

United Kingdom

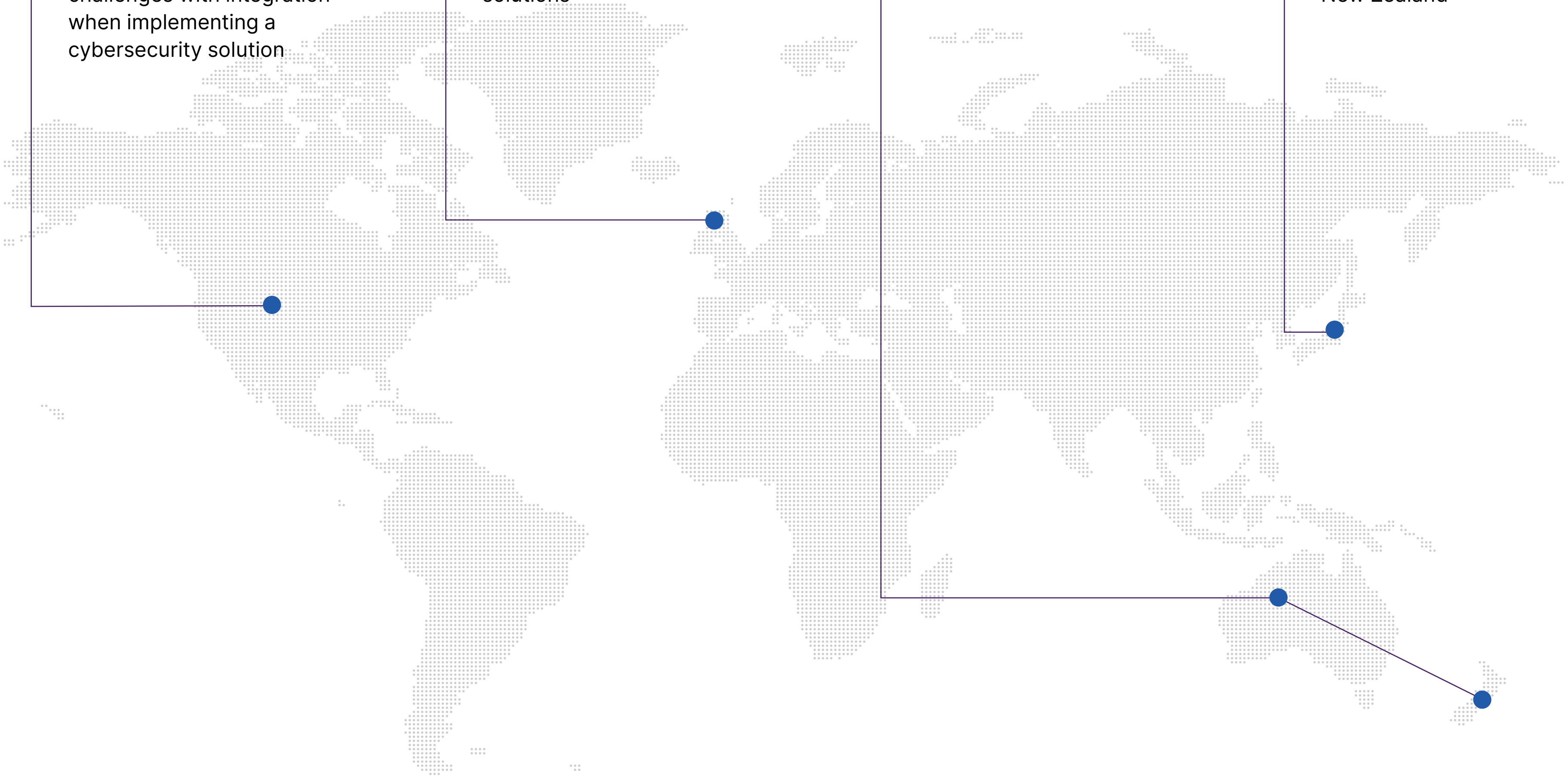
- Most likely to cite incorrect tools as the reason they were unable to prevent a cyberattack in the last 12 months
- More likely than the U.S. and Japan to admit they could do more to prevent attacks by investing in new security solutions

Australia/New Zealand

- Most likely to attribute having failed to prevent a cyberattack in the last 12 months to personal device issues
- Consider lack of strategy the greatest barrier to a technology business' ability to innovate

Japan

- Lowest adoption of AI/ML tools in their cybersecurity strategies
- More likely to have been working with their primary cybersecurity vendor for 5 or more years than counterparts in the U.K. and Australia/ New Zealand



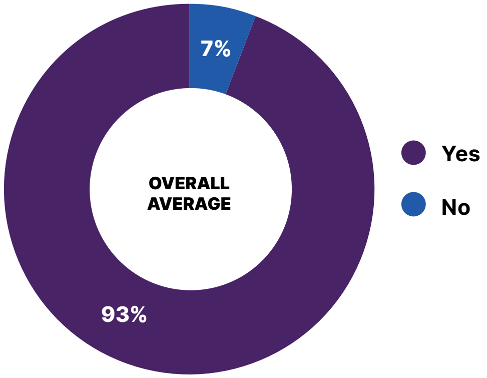
Regional Highlights

CURRENT OUTLOOK

In 2017, when we first surveyed IT decision-makers in the United States and Japan, approximately 74% of businesses were already using some form of AI or ML to protect their organizations from cyber threats, but weren't quite clear what benefits these tools brought.[1] Upon checking in again at the end of 2018, the majority of respondents (72%) agreed that, as long as their protection kept them safe, they didn't care whether it used AI or machine learning; while more than half said they knew they used AI/ML, but weren't sure what that meant.[2] By the end of 2019, a full 96% of respondents, this time distributed across the U.S., U.K., Japan, and Australia/New Zealand, said they used AI/ML tools in their cybersecurity programs, with 68% expressing confusion about their benefits.[3]

Although the percentage has dipped slightly from last year's global average of 96%, a full 93% of global enterprise-level respondents across the U.S., U.K., Japan, and Australia/New Zealand in 2021 say they are already using AI/ML tools in their cybersecurity programs. Additionally, IT decision-makers at these organizations report spending an average of 40% of their cybersecurity tool spend on tools that use AI and/or machine learning.

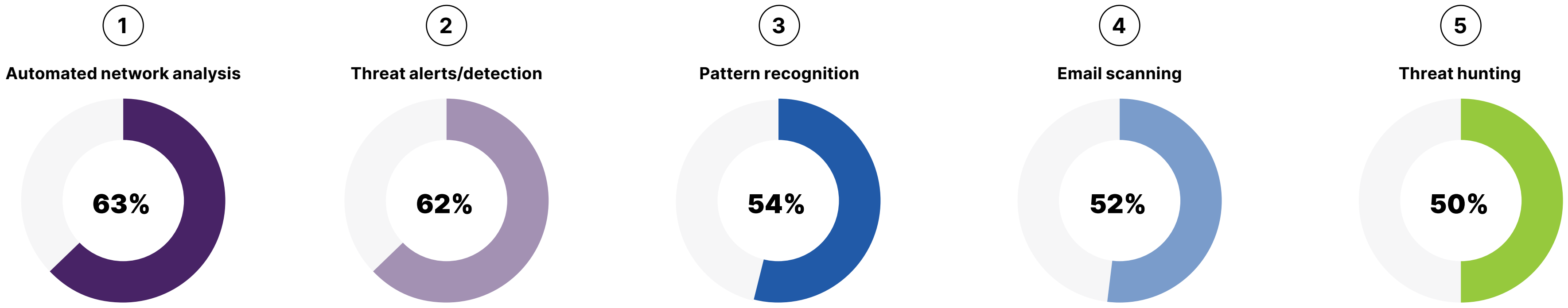
1 *"Do you currently use products with artificial intelligence (AI) or machine learning (ML) capabilities in your cybersecurity program?"*



2 *"Of your total cybersecurity tool spend, how much do you estimate is spent on tools that use AI and/or machine learning?"*

United States	United Kingdom	Japan	Australia/New Zealand
40%	44%	34%	43%

Globally, the top five roles AI and machine learning capabilities play in global cybersecurity programs are:

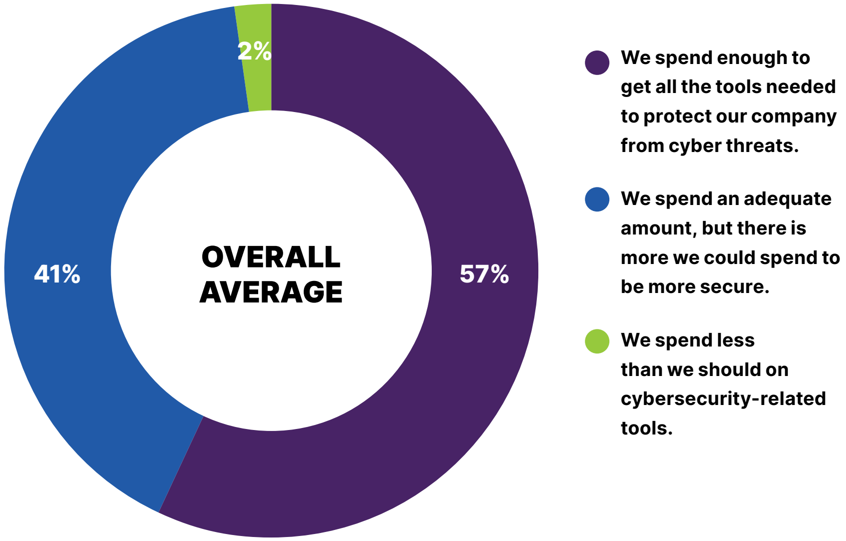


3 *“What role have AI/ML capabilities played in your company’s cybersecurity program?”*

	Overall	United States	United Kingdom	Japan	Australia/New Zealand
Automated network analysis	63%	62%	61%	67%	62%
Threat alerts/detection	62%	61%	66%	66%	58%
Pattern recognition	54%	57%	57%	45%	57%
Email scanning	52%	64%	60%	38%	44%
Threat hunting	50%	49%	50%	55%	49%
User behavior modeling	50%	52%	49%	52%	47%
Employee awareness training	44%	50%	46%	41%	39%
Decrease in response time	37%	41%	35%	47%	25%

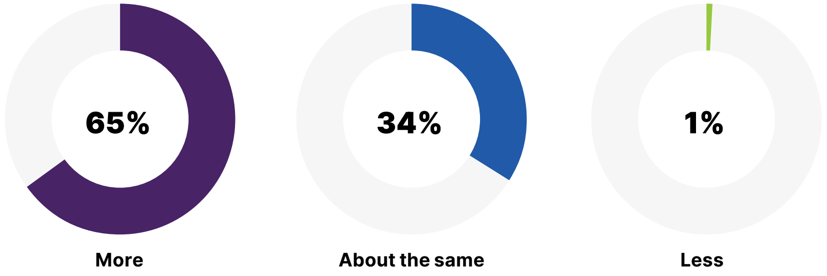
More than half of IT decision-makers surveyed (57%) believe they spend enough to get all the tools needed to protect their company from cyber threats, while approximately four in ten (41%) believe they could be spending more to achieve a stronger level of security.

4 ***“To the best of your knowledge, how would you categorize your company’s current spend on cybersecurity-related tools and services?”***

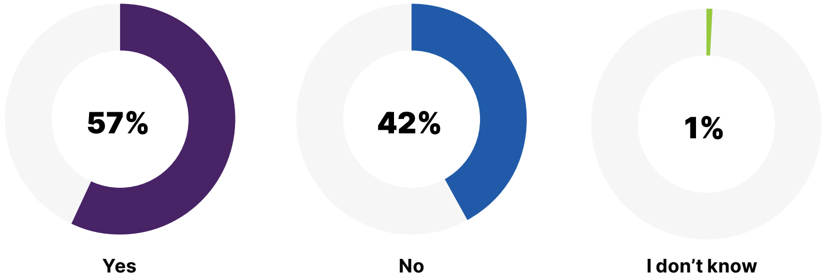


Although the adoption and use of AI/ML-based security tools is high and most (65%) IT decision-makers consider their organizations to be better prepared to handle attacks due to their use of AI and machine learning tools, more than half (57%) of global respondents report they experienced a damaging cyberattack within the last 12 months.

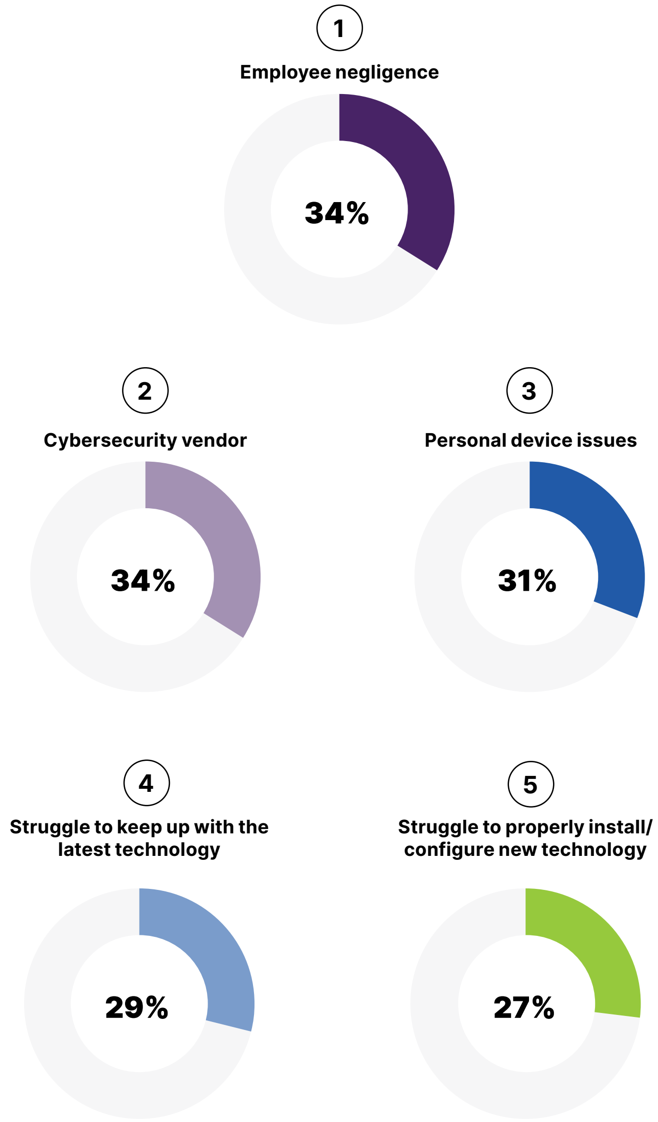
5 ***“Is your organization more or less prepared to handle cybersecurity attacks because it uses AI/machine-learning driven cybersecurity tools?”***



6 ***“Has your organization experienced a damaging cybersecurity attack within the last 12 months despite having cybersecurity tools in place that use AI/machine learning?”***



In a follow-up question that asked respondents to explain why they believed their organizations had been unable to prevent the attacks, the following were their top five responses:



7 *"What do you think are the reasons that your company was unable to prevent the cybersecurity attack?"*

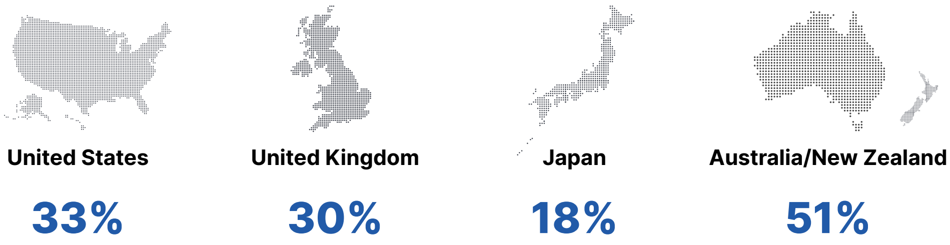
	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Employee negligence	35%	34%	36%	35%	34%
Cybersecurity vendor	34%	35%	39%	24%	38%
Personal device issues	31%	28%	26%	26%	41%
Struggle to keep up with the latest technology	29%	27%	27%	24%	36%
Struggle to properly install/ configure new technology	27%	20%	34%	25%	29%
Inexperienced team	26%	26%	24%	28%	24%
Hardware issue	24%	33%	26%	20%	19%
Lack of CISO/IT team	24%	23%	24%	24%	23%
Lack of training	23%	27%	16%	14%	31%
Lack of support from leadership	22%	21%	20%	23%	22%
Lack of tools	20%	24%	14%	30%	13%
Budget	18%	21%	17%	16%	18%
Not having the correct tools	17%	12%	29%	16%	13%

These figures are slightly different from the responses we received in last year's version of this report; in particular, employee negligence and personal device issues rose higher on the list. We expect these causes correlate directly with the effects of the COVID-19 pandemic and the global shift to working from home.

CONTINUED CONFUSION: YEAR OVER YEAR TRENDS

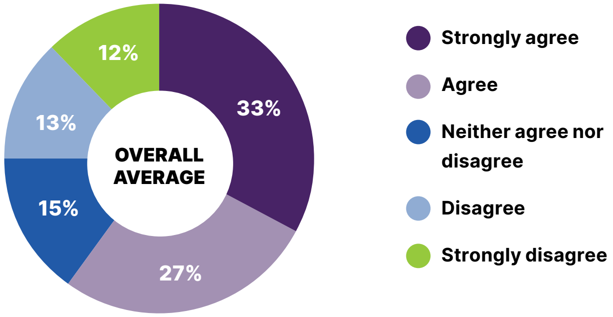
Even though 93% of respondents claim to use cybersecurity tools with AI/ML, IT decision-makers may not be clear on the benefits these tools bring. More than half (55%) of IT decision-makers worldwide agree that, although their tools claim to use AI/ML, they aren't sure what that means.[4] This number is lower than last year's 68%, but still indicates a concerning lack of understanding.

8 ***"How much do you agree with this statement: 'I know some of our tools claim to use AI/ML, but I'm not sure what that means.'?"***

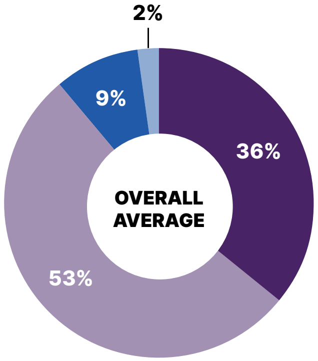


Although 88% of global enterprise IT decision-makers[5] specifically look for vendors who use AI/machine learning, a full 60% of respondents[6] believe cybersecurity vendors are intentionally deceptive about what roles AI/ML play in their products. And yet, when selecting a new cybersecurity tool, 89% consider it important that vendors advertise their use of AI/ML. Last year, these figures were 91%, 70%, and 72% respectively. When taken together, they indicate that confusion about these tools and their benefits, in addition to mistrust of vendors, is slowly lessening, while the proportional understanding of their importance, at least, is on the rise.

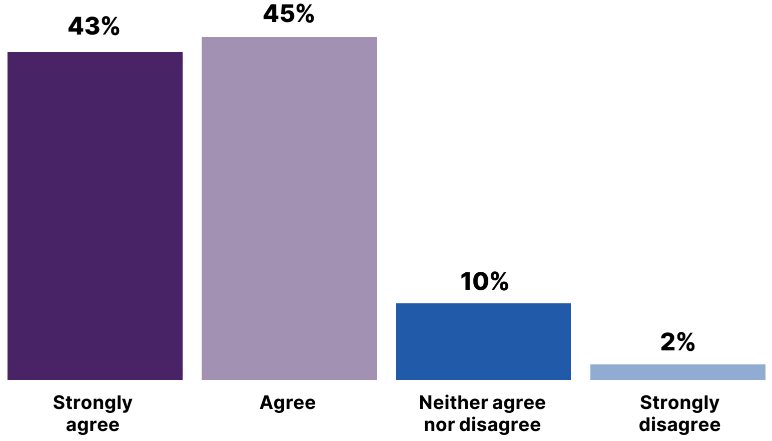
9 ***"How much do you agree with this statement: 'I think cybersecurity tool vendors are being purposefully deceptive when it comes to how they market their AI/ML cybersecurity tools.'?"***



10 ***"How much do you agree with this statement: "'It is important that the manufacturer advertises its use of AI or machine learning applications to deliver its service.'"***



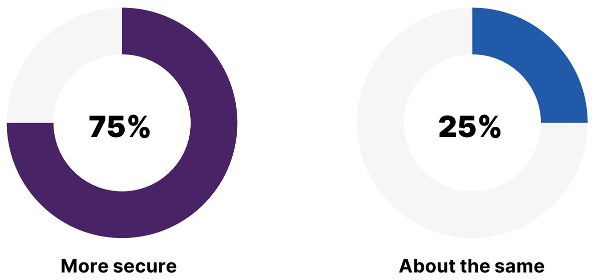
11 *"How much do you agree with this statement: 'I understand and research the cybersecurity tools we use and specifically look for ones that use AI/ML to protect my organization.'?"*



OVERALL AVERAGE

As a further continuation of the trend of confusion, while 55% say they aren't sure what AI/ML brings their organizations, 75% say their organizations are more secure due to their use of AI/ML cybersecurity tools (down from 77% in our previous survey). And yet, 62% say that, as long as those tools are effective in stopping cyberattacks, they don't care if those tools use AI or machine learning (down from 74%).

12 *"Do you think your organization is, or would be, more secure due to its use of AI and/or machine learning cybersecurity tools?"*



OVERALL AVERAGE

13 *"How much do you agree with this statement: 'As long as the tools we use help protect us against cybercriminals and other cyber threats, I don't care if it uses AI/ML.'?"*

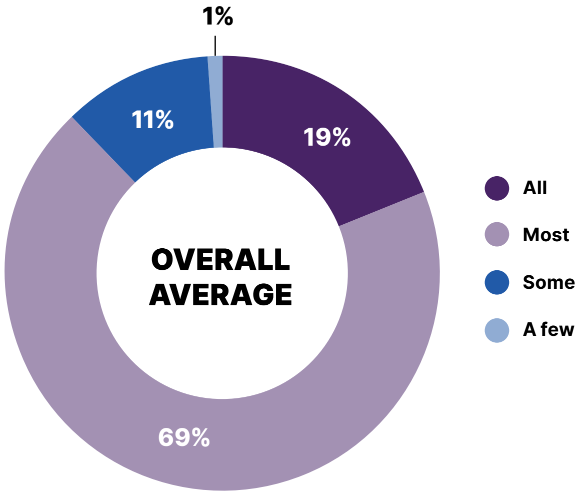
	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Strongly agree	27%	28%	32%	18%	31%
Agree	35%	32%	34%	33%	39%
Neither agree nor disagree	21%	19%	17%	30%	20%
Disagree	12%	13%	12%	12%	10%
Strongly disagree	6%	9%	6%	8%	2%

As we examine these differences, they indicate enterprise IT decision-makers' desire to use whatever means are necessary to effectively protect their organizations, even if it means embracing technologies whose inner workings and benefits aren't apparent.

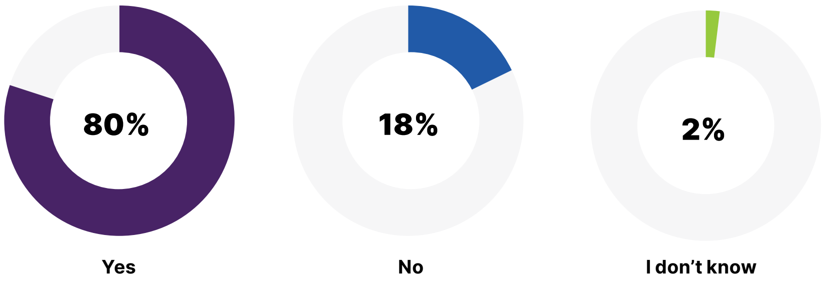
THE REALITY OF THE THREAT LANDSCAPE

It’s clear from the responses we received that organizations believe they’ve been harder hit by cyberattacks in the last year than in years prior. Throughout the globe, just 19% of IT decision-makers say their current tools help stop all of their cybersecurity-related threats, compared with 36% in our previous survey. Meanwhile, the number of organizations who are certain they could be doing more to prevent attacks is holding relatively steady year-over-year, down to eight in ten (80%) from last year’s 86%.

14 *“Please select one response that fills in this blank: “Our tools help stop ______ of our cybersecurity-related threats.”*



15 *“Do you think there is more your company could be doing to better defend against cybersecurity attacks?”*

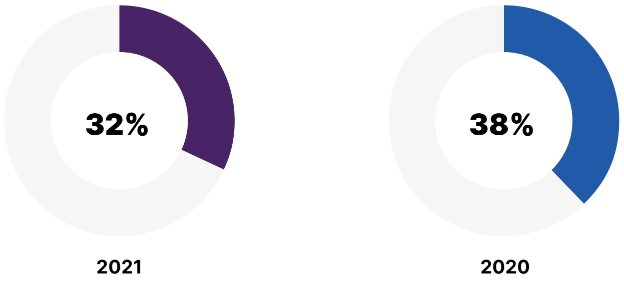


OVERALL AVERAGE

When asked what their company could do to better defend against cybersecurity attacks, the top three answers remained the same as last year:

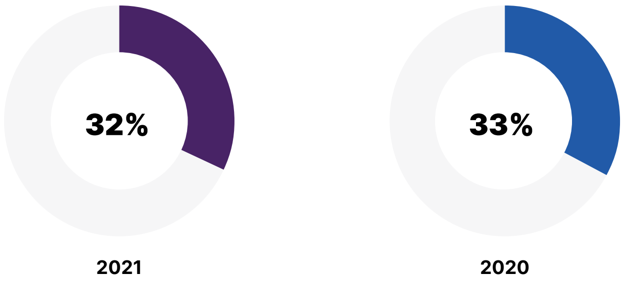
1

Investing in AI/machine learning-based cybersecurity solutions



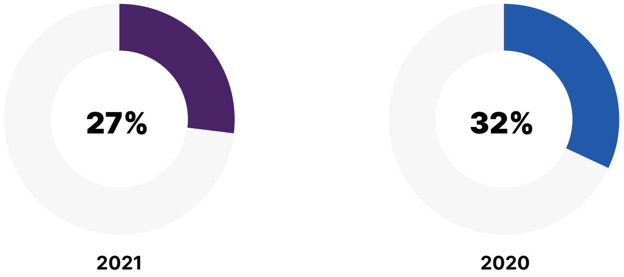
2

Security awareness training



3

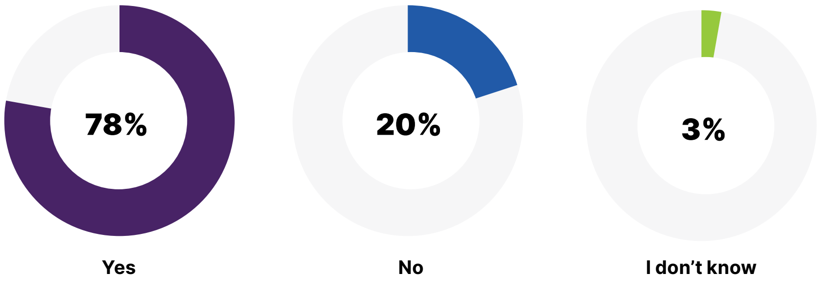
Investing in new security software



16 *"What could your company be doing better to defend against cyberattacks?"*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Invest in AI/machine learning-based cybersecurity solutions	32%	32%	26%	43%	29%
Security awareness training	32%	34%	30%	35%	30%
Invest in new security software	27%	21%	35%	16%	34%
Monthly or quarterly security review of protocols or program checklist	22%	21%	22%	22%	22%
Hire more IT staff	19%	25%	22%	18%	13%
Support from leadership	19%	15%	16%	17%	28%
Purchase new equipment	17%	20%	15%	18%	14%
Hire a CISO (Chief Information Security Officer)	14%	15%	16%	14%	13%
Incentive-based learning	14%	13%	15%	13%	16%

17 *"Do you think your organization has everything it needs to successfully defend against AI/ML-led cybersecurity attacks?"*



OVERALL AVERAGE

AGE VS. INNOVATION FOR BUSINESS CONTINUITY

Although there's a widespread belief that younger companies can bring innovative technology to market faster than their older counterparts, global enterprise IT decision-makers report a preference towards greater experience when working with primary cybersecurity vendors at their organizations.

Four in five enterprise IT decision-makers (83%) believe age positively impacts a technology business' ability to innovate.

18 *"In your opinion, does the age of technology business' impact its ability to innovate?"*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Age positively impacts a technology business' ability to innovate.	63%	62%	61%	67%	62%
Age somewhat positively impacts a technology business' ability to innovate.	62%	61%	66%	66%	58%
Age does not have an impact on a technology business' ability to innovate.	54%	57%	57%	45%	57%
Age somewhat negatively impacts a technology business' ability to innovate.	52%	64%	60%	38%	44%
Age negatively impacts a technology business' ability to innovate.	50%	49%	50%	55%	49%

Overall, companies are largely turning to vendors with experience. Four in ten respondents (41%) whose organizations use AI or machine learning capabilities in their cybersecurity program say their primary cybersecurity vendor is between six and ten years old. Additionally, 16% report their primary cybersecurity vendor being 11-20 years old, while 9% estimate their primary cybersecurity vendor is over 20 years old.

19 *"To the best of your knowledge, how old is the primary cybersecurity vendor your organization works with (age meaning from founding date to present)?"*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Less than 3 years old	5%	7%	6%	1%	5%
3-5 years old	27%	31%	33%	10%	33%
6-10 years old	41%	35%	36%	55%	40%
11-20 years old	16%	18%	12%	18%	16%
Over 20 years old	9%	8%	11%	14%	3%
I don't know	2%	2%	2%	2%	3%

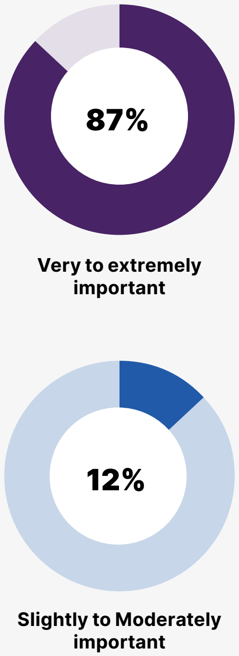
Not only are organizations working with experienced cybersecurity companies, but they are also retaining these relationships. Over one third of survey respondents whose organizations use AI or ML capabilities in their cybersecurity program say their organization has been working with their primary cybersecurity vendors for one to two years (36%) or three to four years (37%). Only 8% report working with their primary cybersecurity vendor for less than 1 year.

20 *"How long has your organization been working with its primary cybersecurity vendor?"*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Less than 6 months	1%	2%	1%	1%	1%
6-11 months	7%	8%	11%	3%	6%
1-2 years	36%	32%	42%	31%	37%
3-4 years	37%	35%	29%	38%	44%
5 or more years	20%	23%	17%	27%	13%

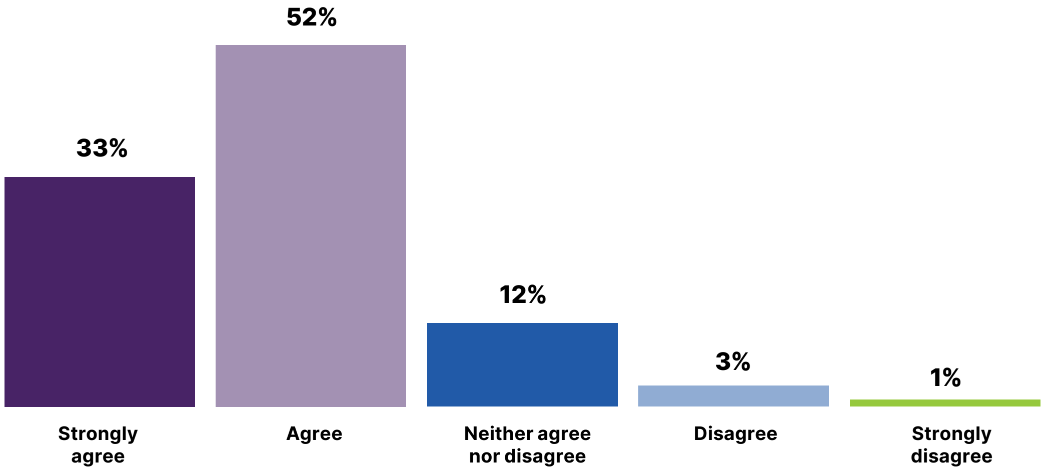
Globally, these figures indicate that organizations recognize how age can be an asset in AI-enabled technology. Nearly nine in ten respondents (87%) say the age of AI systems is very-to-extremely important in their decision making and selection when evaluating new AI-enabled technology for their organization. However, nearly half of respondents (49%) consider it more important that their tools update often, regardless of the age of the vendor providing them.

21 ***"When evaluating new AI-enabled technology for your organization, how important is the age of their AI system in your decision making and selection?"***



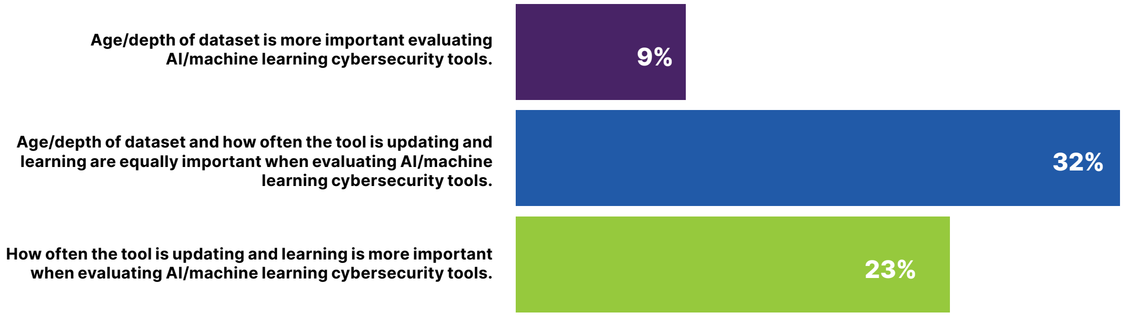
OVERALL AVERAGE

22 ***"Please indicate your level of agreement with the following statement: Theoretically, if two AI systems have similar inputs but one AI system has had more years to learn than the other, the older one will be smarter."***



OVERALL AVERAGE

23 ***"When evaluating AI/machine learning cybersecurity tools, what best describes your organization's view of age/depth of the dataset and how often the tool updates or learns?"***

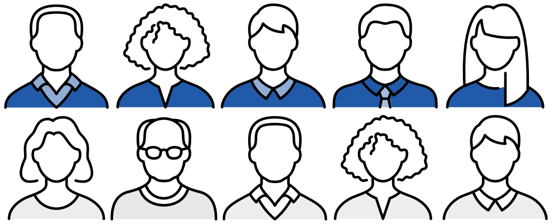


OVERALL AVERAGE

When considered against the figures presented in the previous section regarding how well IT decision-makers understand their tools and their efficacy, the factor of age indicates a level of trust in older, more experienced vendors. By choosing more experienced vendors, enterprises may feel more confident in their cybersecurity programs and ability to ensure business continuity, even if they don't fully understand the tools they use or their capabilities.

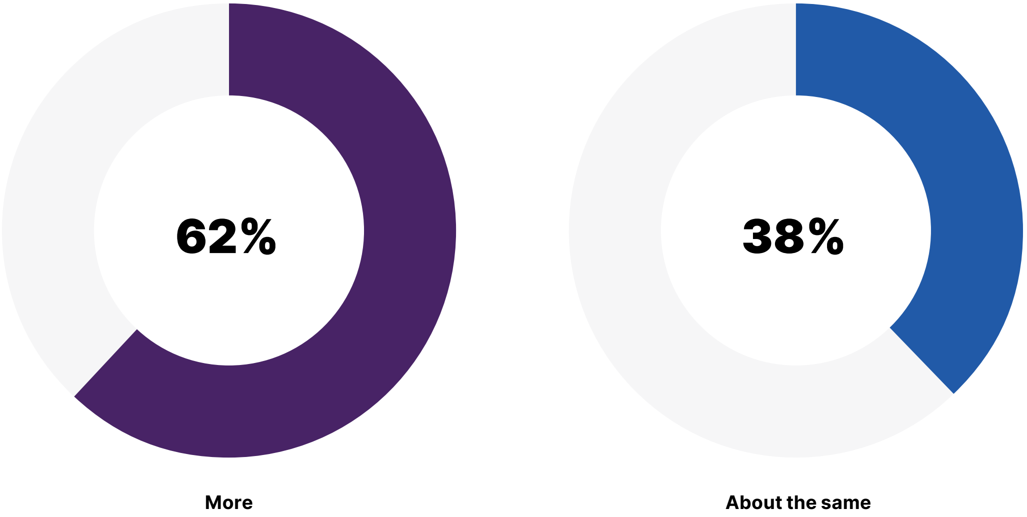
FUTURE OUTLOOK

From the data, most enterprise IT decision-makers believe using AI and machine learning in cybersecurity is an essential part of addressing current and future threats. Although the percentage is lower than last year's seven in ten, approximately six in ten (62%) of respondents plan to increase their use of AI/ML cybersecurity tools in 2021.



Nearly half (47%) of enterprise IT decision-makers plan to focus on increased AI or machine learning adoption in 2021.

24 *"Does your organization plan to use more or fewer AI/ML cybersecurity tools in 2021?"*

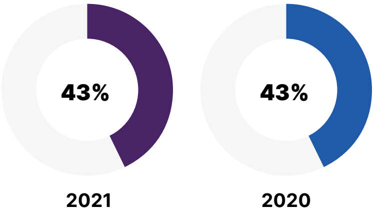


OVERALL AVERAGE

When asked which areas they believe their organizations should focus on to successfully defend against AI/ML-based cyberattacks, global IT decision-makers listed the following as their top five, holding fairly steady with last year's values:

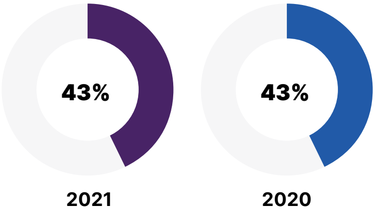
1

New cybersecurity tools or solutions



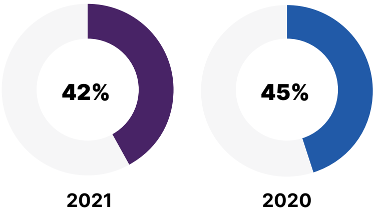
2

Upgrading IT infrastructure



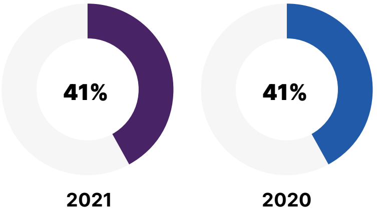
3

Increased training or awareness of IT employees



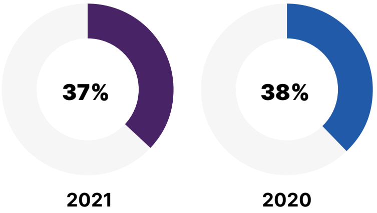
4

General IT security budget increases



5

Increased training or awareness of general employees



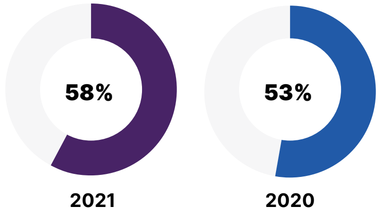
25 ***“What are some areas that your organization needs to focus on to successfully defend against AI/machine learning led cybersecurity attacks?”***

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
New cybersecurity tools or solutions	43%	47%	45%	37%	45%
Upgrading IT infrastructure	42%	44%	47%	39%	39%
Increased training or awareness of IT employees	42%	43%	40%	42%	41%
General IT security budget increases	41%	43%	40%	42%	41%
Increased training or awareness of general employees	37%	40%	33%	37%	37%
New hires for specific cybersecurity skills	36%	33%	35%	43%	34%
Better internal policies and procedures	35%	36%	33%	29%	41%
Participate in industry and government data sharing	25%	19%	30%	26%	25%

In a related question, the need for cybersecurity/infrastructure upgrades and training for staff were highlighted again and again. The top five areas in which respondents reported they plan to increase investment also held steady with values from our previous survey, with the exception of increased training (41% previously; now down to 33%):

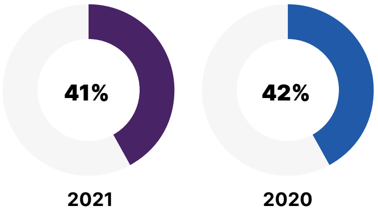
1

Cybersecurity



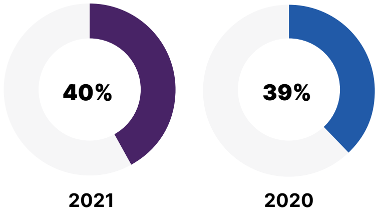
2

Threat intelligence



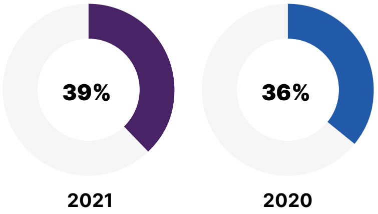
3

Software



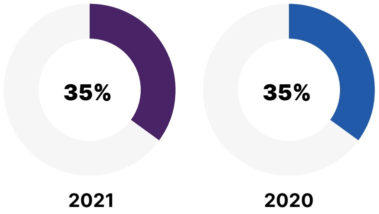
4

Data storage and management



5

Infrastructure

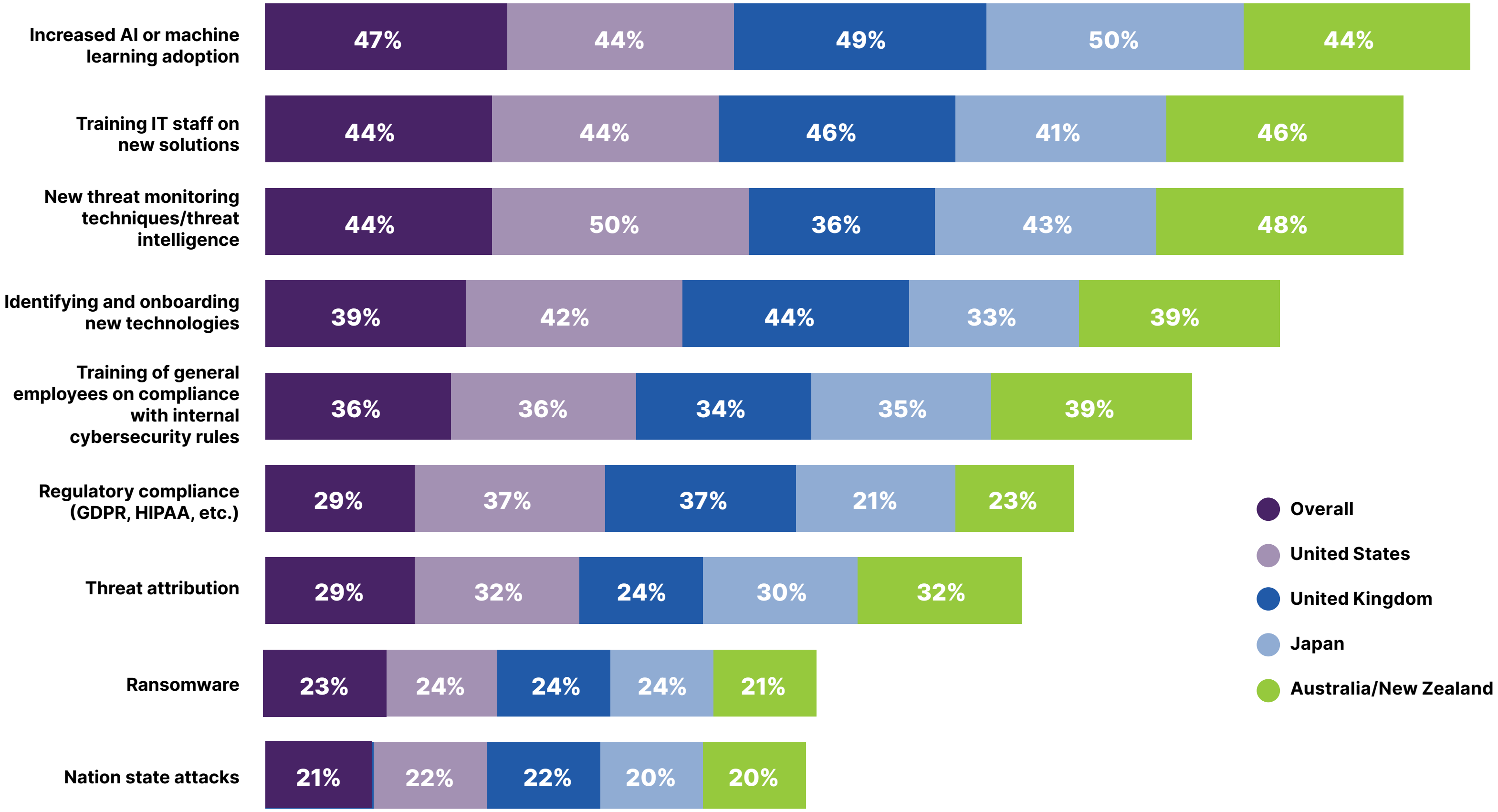


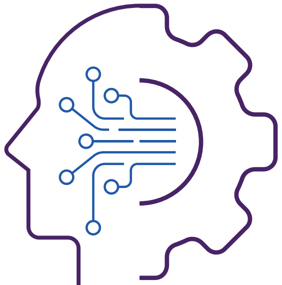
26 *"In what IT areas does your organization plan to increase investment 2021?"*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Cybersecurity	58%	67%	55%	53%	57%
Threat intelligence	41%	47%	37%	38%	42%
Software	40%	45%	41%	34%	42%
Data storage and management	39%	41%	38%	43%	35%
Infrastructure	35%	37%	37%	34%	34%
Increased trainings	33%	35%	29%	33%	38%
Email security	31%	34%	31%	32%	29%
Endpoints (computers, tablets, phones, etc.)	30%	33%	36%	26%	25%
New staff	23%	21%	22%	25%	25%

Additionally, when asked which cybersecurity-related areas they specifically planned to focus on in 2021, IT decision-makers reported the same top three categories, with minor shifts in order of importance, namely increased AI or machine learning adoption, more training for IT staff, and new threat monitoring techniques/threat intelligence.

27 *“Thinking about your organization’s cybersecurity plans for 2021, what are the biggest areas you plan to focus on?”*





Key Takeaways for Enterprises

Understanding is increasing, but still too low.

It’s important to educate internal teams, end users, and customers (as applicable) on the benefits of AI/ML and their role in cybersecurity, so you can realize the maximum return on your cybersecurity investments.

AI/ML are increasingly necessary for resilience against modern threats.

No matter what business you’re in, your customers expect a high level of service. As attacks become more sophisticated, advanced technologies that use AI and ML will be among the only ways to effectively combat threats and ensure uptime and availability for your business and customers.

Using AI/ML in your products and cybersecurity programs can differentiate your business.

Whether customers fully understand the benefits of AI/ML, it’s clear businesses and individuals are beginning to realize the necessity of using such tools. Incorporating AI/ML-enabled security into your own products and/or cybersecurity programs can help you differentiate your service offerings from your competitors.

SMALL & MEDIUM-SIZED BUSINESSES

<250 EMPLOYEES

Regional Highlights

United States

- Most value the ability to protect against the latest cybersecurity threats when vetting new vendors
- Reported the lowest increases in the number of cyberattacks faced since the COVID-19 pandemic began

United Kingdom

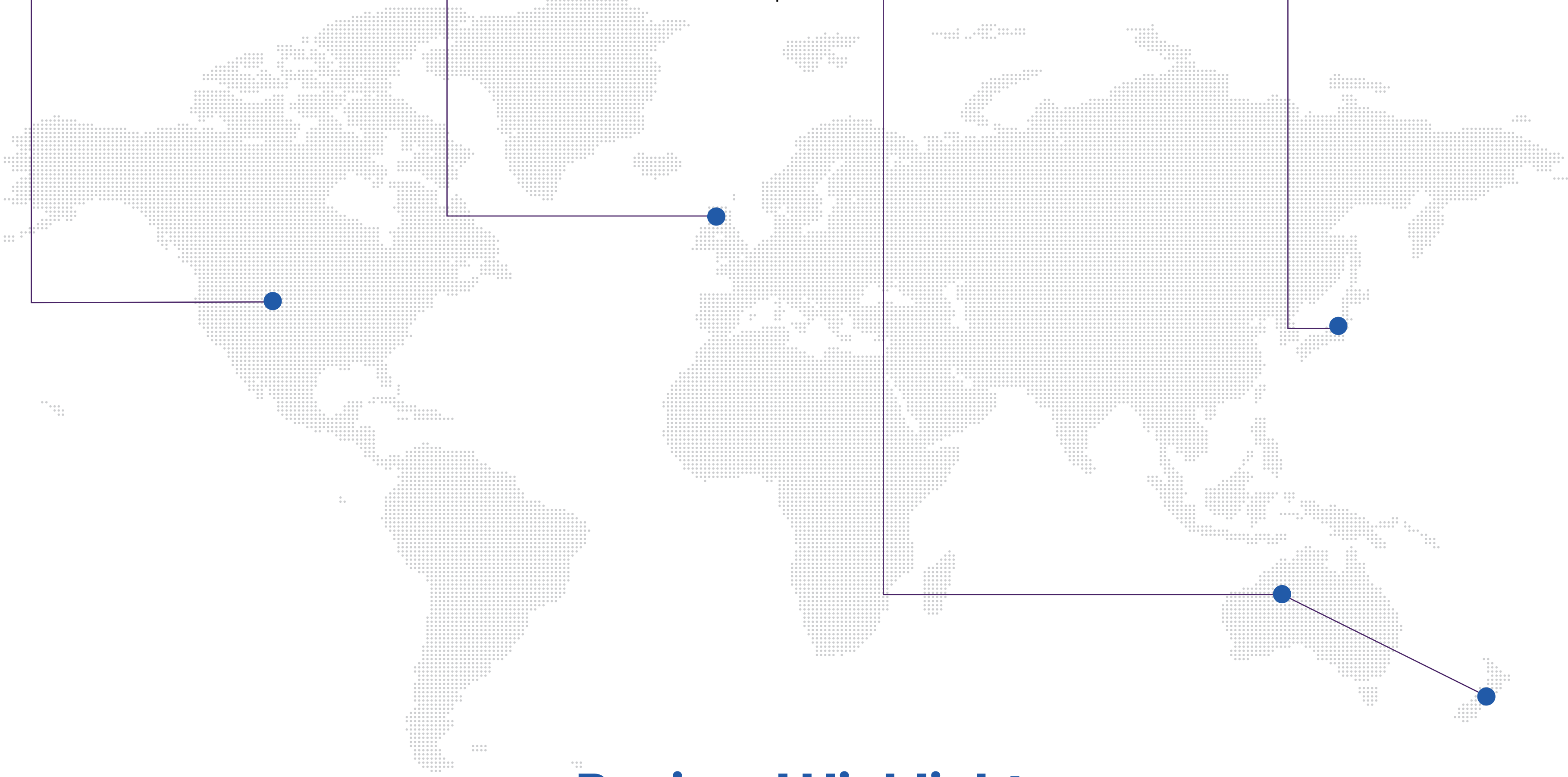
- More likely to report that their business’ data has never been stolen or breached than counterparts in Australia/New Zealand and Japan
- More likely to use antivirus or antimalware protection on company devices compared to Australia/New Zealand and Japan

Australia/New Zealand

- Most likely to claim knowledge or understanding of AI/ML
- More concerned their business could experience a cyberattack or data breach compared to other geographies

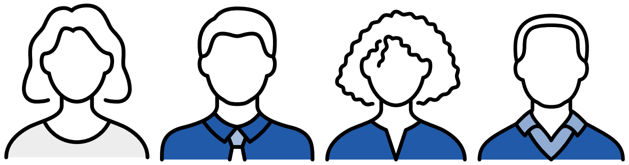
Japan

- More likely to say they only use the security provided by their cloud services to protect the data they store in the cloud compared to Australia/New Zealand the U.S.



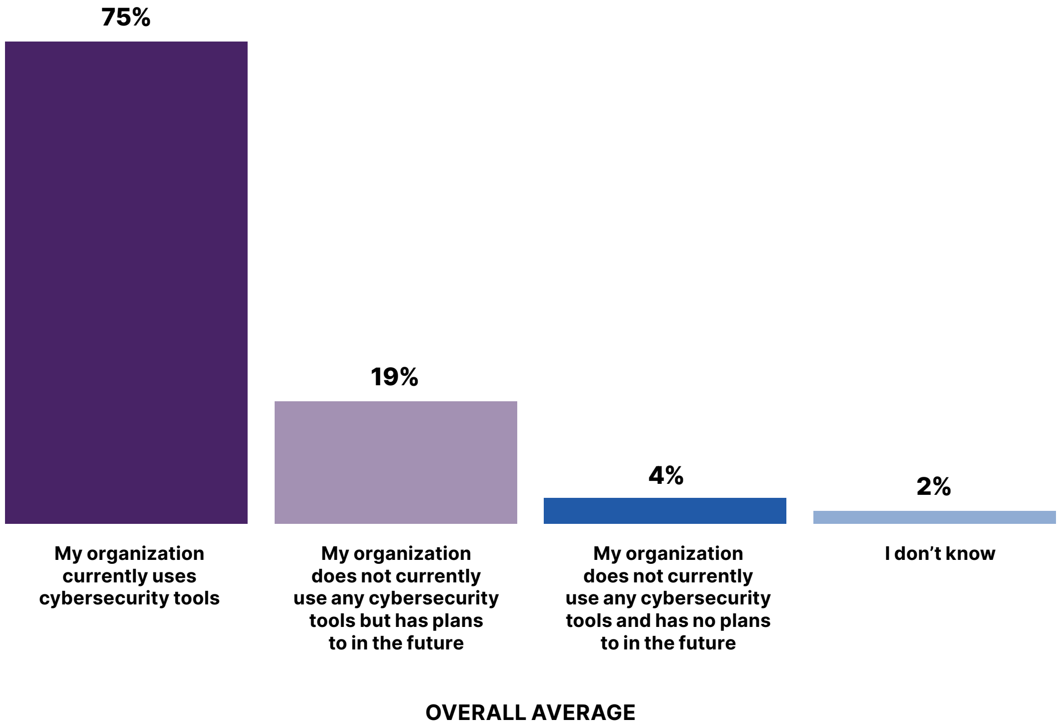
CURRENT OUTLOOK

Although we've published the findings from this survey annually, this is the first year we surveyed audiences outside of the enterprise (1000+ employees) space. Small and medium-sized businesses (SMBs) traditionally comprise of organizations with 250 employees or fewer and often have different concerns and conceptions when it comes to their security than their larger counterparts.



Three out of four (75%) SMB IT decision-makers surveyed say their organizations use cybersecurity tools.

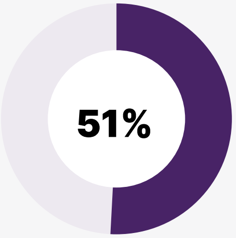
28 *"Does your organization currently use any cybersecurity tools?"*



Interestingly, while three in four say they use cybersecurity tools, only about half report taking precautions like using antivirus or antimalware software on company devices. The top three security precautions SMBs take are:

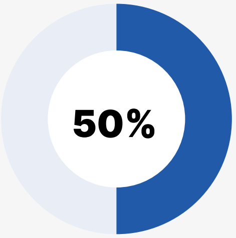
1

Regularly backing up company data



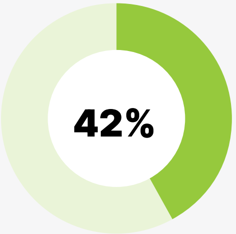
2

Using antivirus or antimalware protection on company devices (e.g., computers, phones, etc.)



3

Installing software updates on company devices regularly

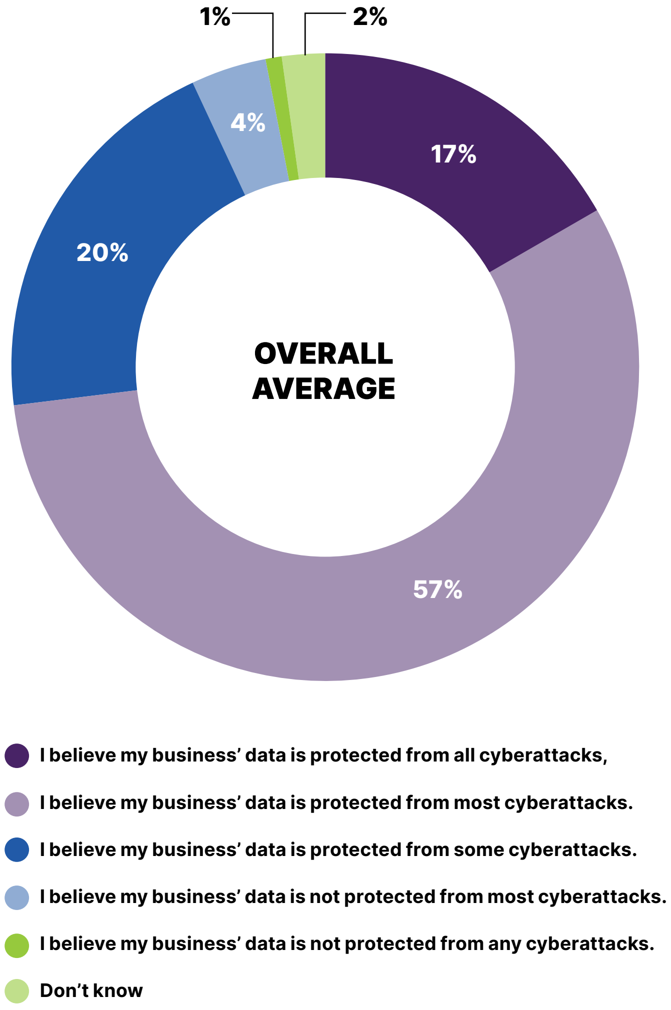


29 *“Does your business take any of the following cybersecurity precautions?”*

	Overall	United States	United Kingdom	Japan	Australia/ New Zealand
Regularly backing up company data	51%	60%	51%	46%	47%
Using antivirus or antimalware protection on company devices (e.g., computers, phones, etc.)	50%	59%	54%	44%	44%
Installing software updates on company devices regularly	42%	49%	46%	33%	41%
Requiring employees and company accounts to change passwords every 30-90 days	39%	38%	41%	33%	43%
Requiring employees to use/Using different passwords for every platform/account	37%	33%	39%	38%	36%
Requiring employees to use/Using Two-factor or Multi-factor Authentication (MFA)	33%	34%	34%	31%	35%
Requiring employees to use/Using a VPN	29%	29%	29%	26%	32%
Requiring employees to use/Using an email account-enabled password-manager (e.g., iCloud keychain, Google password manager)	29%	28%	26%	27%	34%
Monthly or quarterly security review of protocols or program checklist	27%	32%	26%	24%	28%
Requiring employees to use/Using a password-manager vendor/subscription (e.g., LastPass, Keeper, Dashlane, 1Password, Bitwarden, etc.)	25%	25%	19%	25%	31%

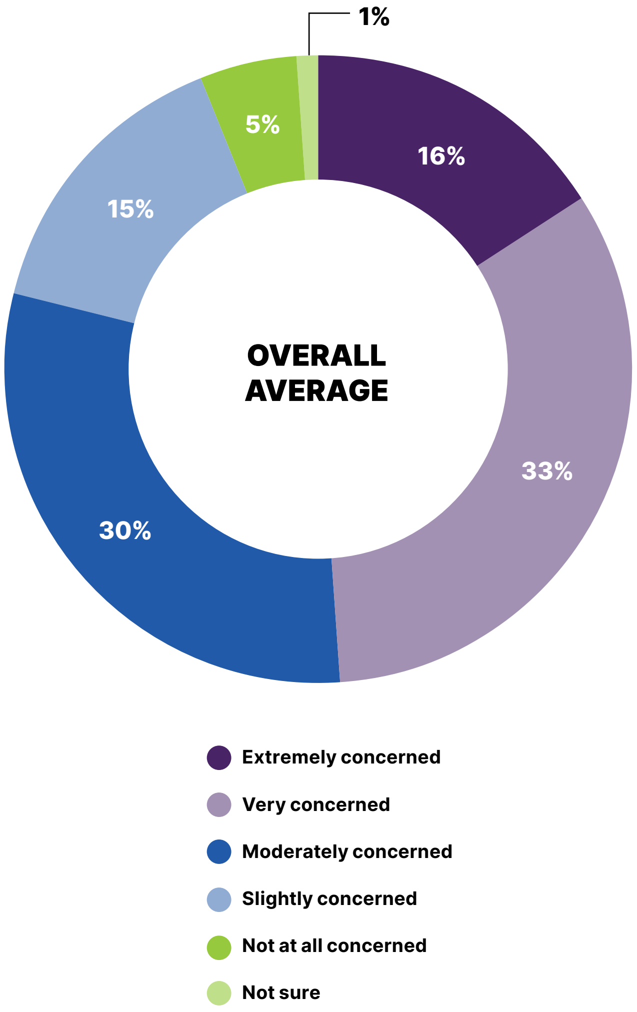
SMBs largely consider themselves protected against cyberattacks, with a full 74% reporting they believe their data is protected from most or all cyberattacks. A further 20% consider themselves safe from some cyberattacks, while 7% are unsure or believe they could be at risk.

30 *"Do you believe that your business' data is protected from cyberattacks?"*



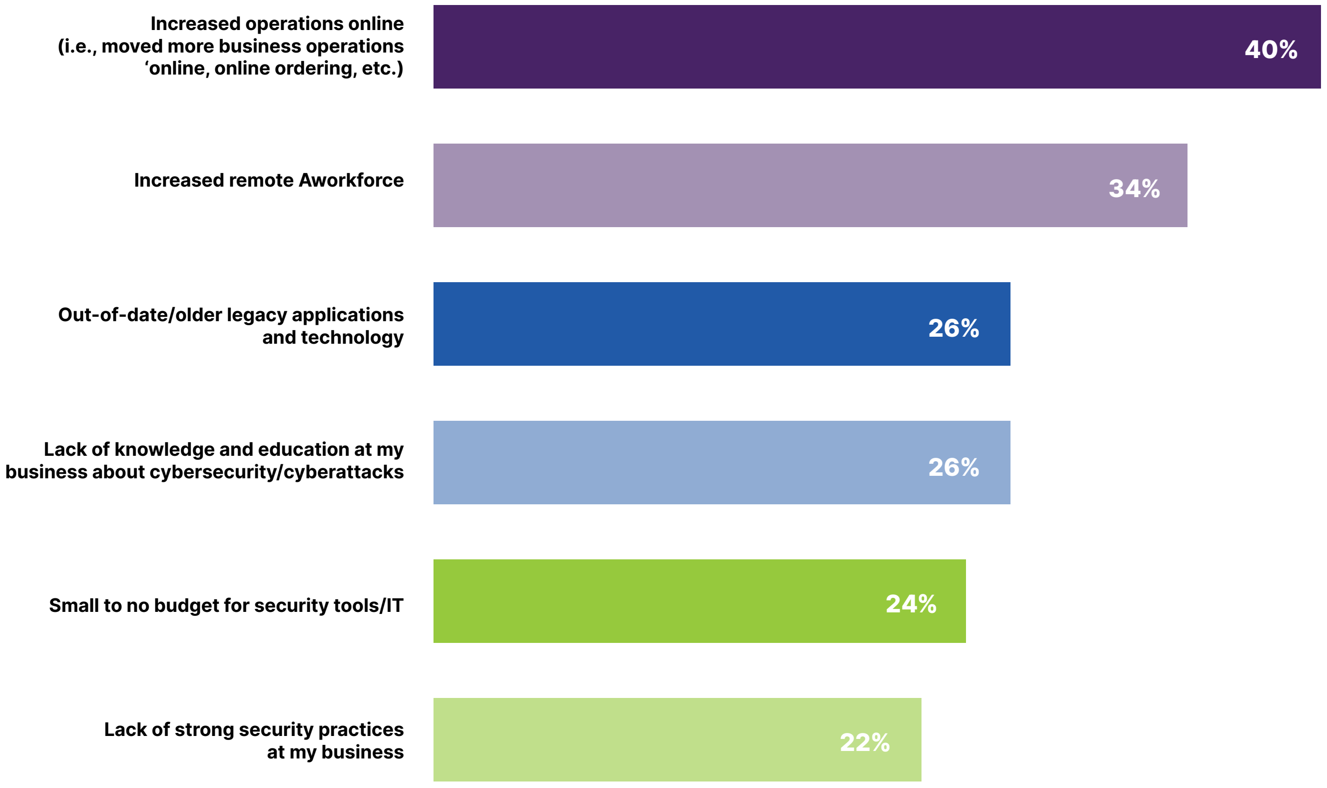
Globally, 79% of SMB IT decision-makers are moderately to extremely concerned that their business could experience a cyberattack. The majority attribute their concern to increased operations online, increased remote workforce and out-of-date, older legacy applications and technology, and lack of adequate knowledge or training.

31 *"Are you concerned that your business could experience a cyberattack or data breach?"*



These concerns align with a general notion that all businesses are vulnerable to some form of attack (more on this in the next section), despite a small number of respondents admitting they are not worried about cyber threats.

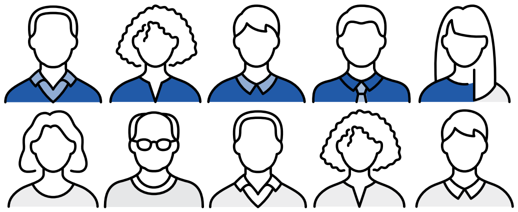
32 *"Why are you concerned that your business could experience a cyberattack or data breach?"*



OVERALL AVERAGE

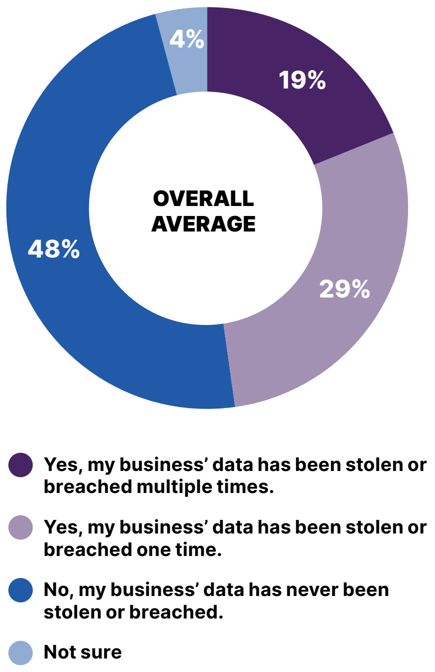
THE REALITY OF THE THREAT LANDSCAPE

Nearly half of SMBs have had their data stolen or breached at least once. However, an equal number claim their data has never been exposed, while a further 4% aren't sure whether they have been compromised or not. Additionally, nearly one-third of respondents noticed changes in the number of attacks during the COVID-19 pandemic; while 38% claim to have experienced the same number of attacks during the pandemic as they had previously, an additional 40% reported an increase in attacks.

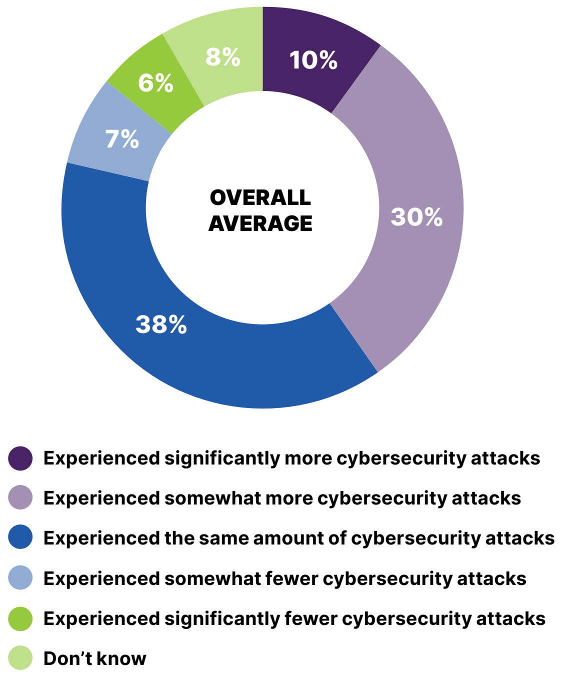


Almost half of SMBs (48%) say their business' data has been stolen or breached at least once.

33 ***"Are you aware if your business' data has ever been stolen or breached?"***

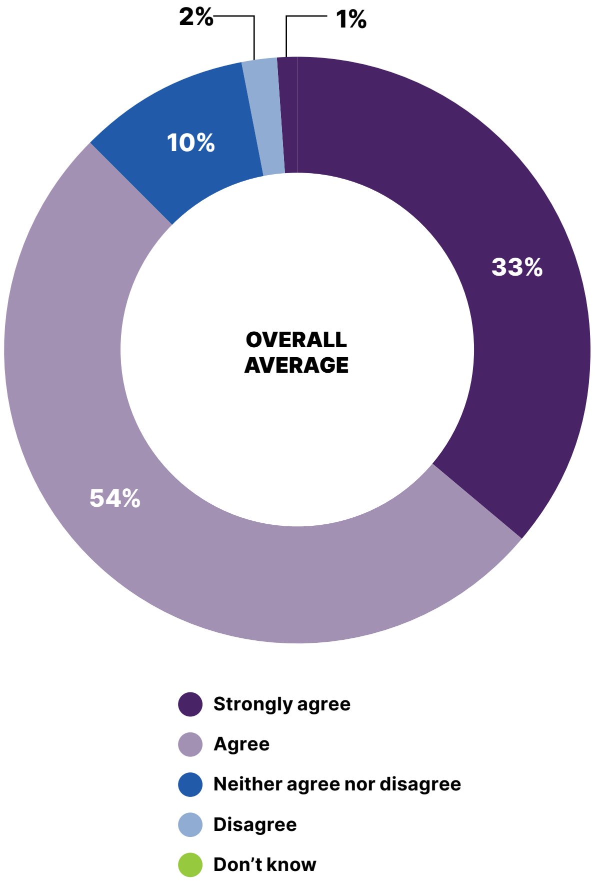


34 ***"Has the number of cybersecurity attacks your business has experienced changed since the COVID-19 pandemic began?"***

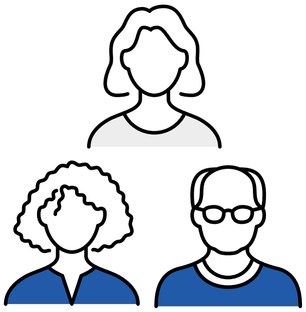


Given the increasing number of stealth cyberattacks that operate under the radar, gathering intel for weeks or months before visible signs of the attack appear, our experts consider the 48% who claim their data has never been breached to be overly optimistic. It's also unlikely that respondents truly believe their own estimates; nearly nine out of ten respondents (87%) either agree or strongly agree that all businesses are vulnerable to attacks, regardless of any protections they may have in place.

35 *"Please indicate your level of agreement with the following statement: At some level, all businesses are vulnerable to cyberattacks despite any protections that may have been put in place."*

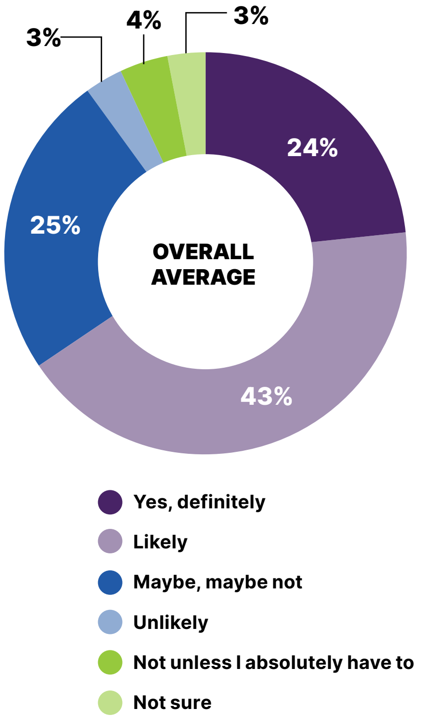


It's possible that some businesses are not aware if their data may have been breached through a supply chain attack on one of the vendors they do business with. However, most SMBs (67%) consider a supply chain breach to be reason enough to terminate (or strongly consider terminating) their working relationship with that vendor.



Two in three SMBs say they would likely or definitely stop working with a platform or service if their data were compromised through that platform.

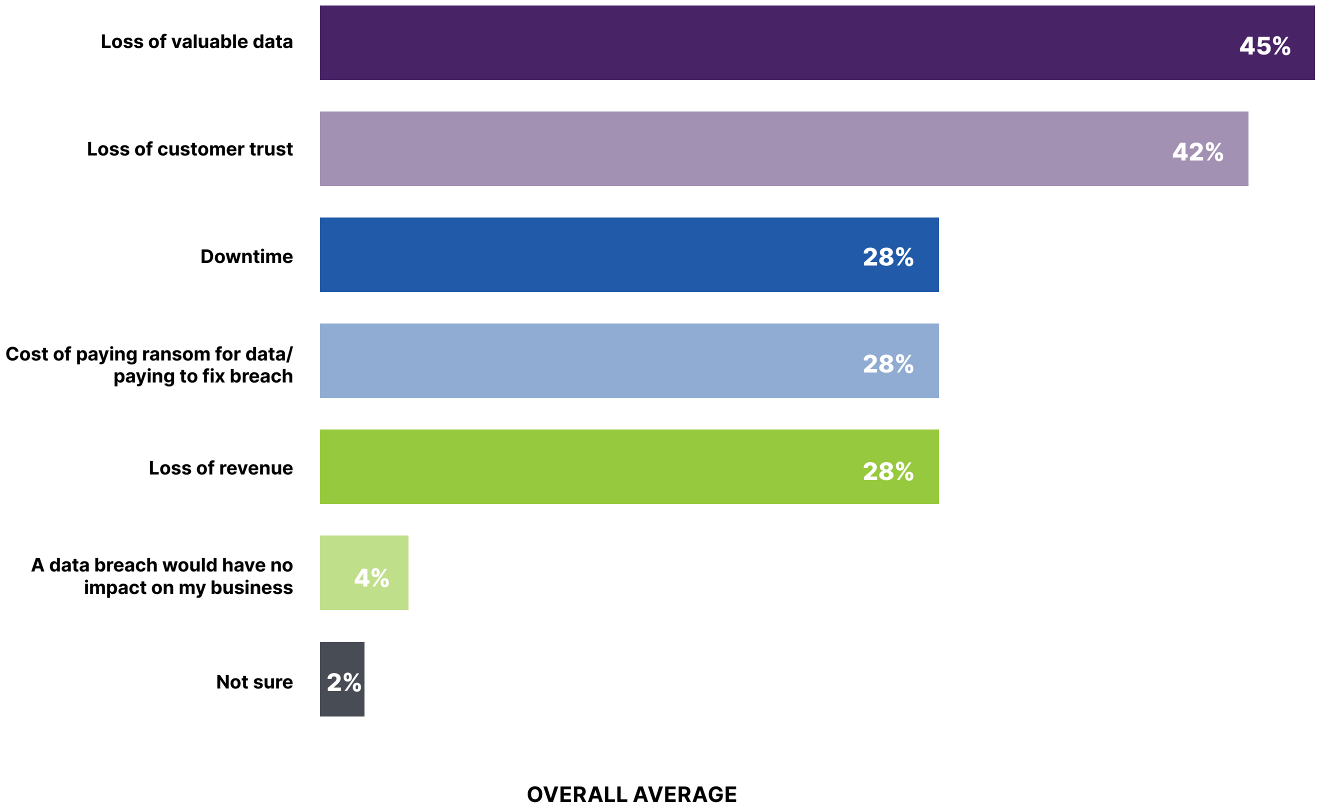
36 *"If your business' data had been exposed or stolen through a platform/service you use, would you stop using or working with that platform/service?"*



More than one-third of SMBs (37%) who use the cloud to store their business' data report they only use the security provided by their cloud services to protect their data, indicating a strong reliance on their vendor partners to keep their critical business data safe. And when we consider the self-reported impacts of a small or medium-sized business' data breach, it's easy to see why some might consider the security of their vendor partners a non-negotiable must.

Overall, SMBs list loss of valuable data (45%) and loss of customer trust (42%) as the biggest impacts of a cybersecurity breach, both of which can easily lead to bankruptcy, if the business suffers too much subsequent downtime or loss of business.

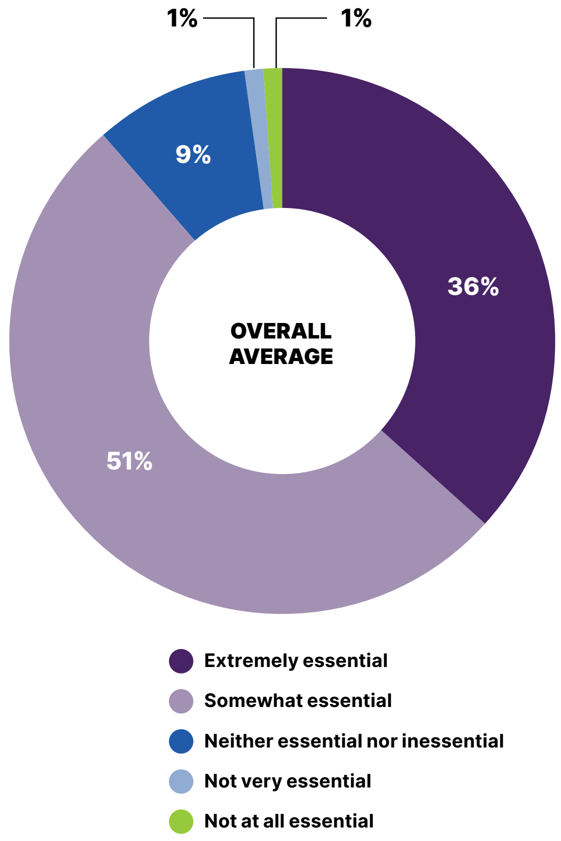
37 *"What kind of impact, if any, would a data breach have on your business?"*



FUTURE OUTLOOK

Considering their reliance on a vendor partners' security, SMBs must look for solutions that use the latest technology and security practices to protect their critical data. In particular, 87% of IT decision-makers at small and medium-sized businesses consider the use of AI and machine learning somewhat to extremely essential for addressing cyber threats.

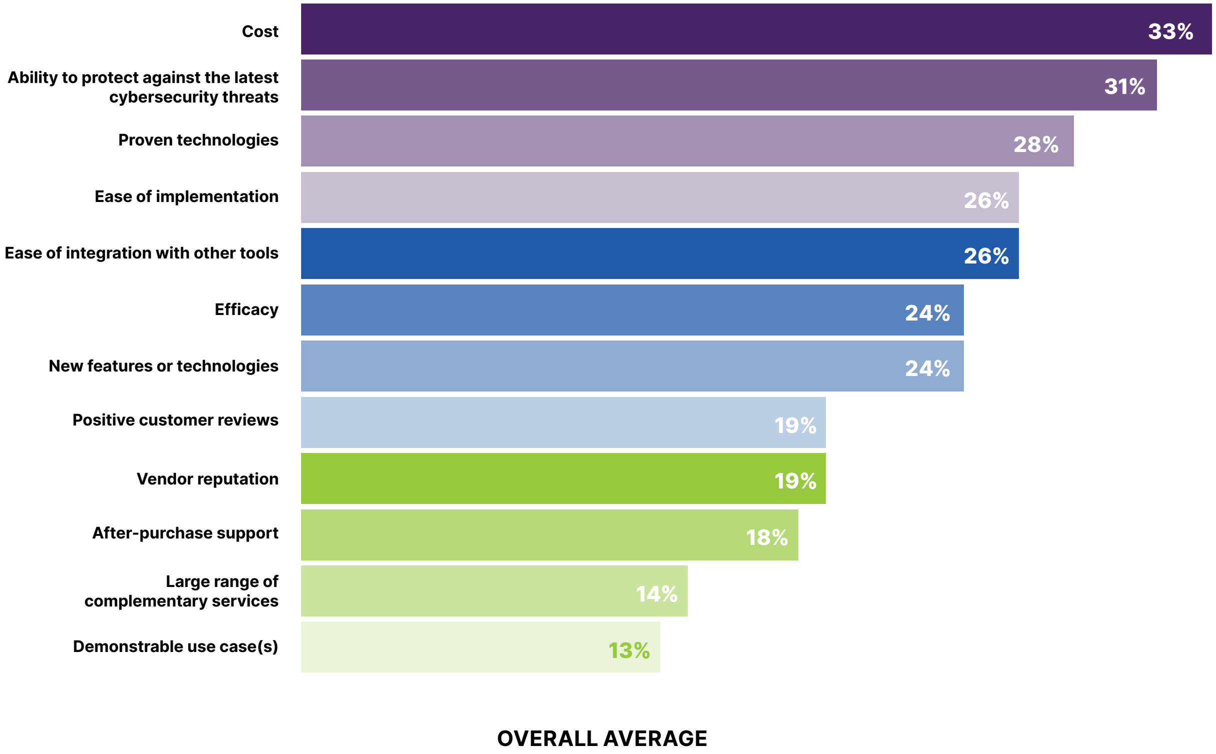
38 *"How essential is the use of AI and machine learning in addressing current and future security threats?"*



When choosing a vendor, SMBs cite the following qualities as their top five features to look for:

- Cost (33%)
- Ability to protect against the latest cybersecurity threats (31%)
- Proven technologies (28%)
- Ease of implementation (26%)
- Ease of integration with other tools (26%)

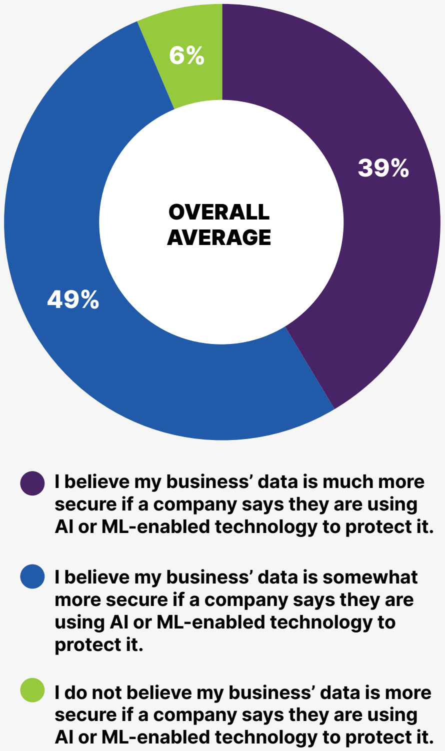
39 *"When choosing a technology solution/technology vendor, what are the most important features that your company looks for?*

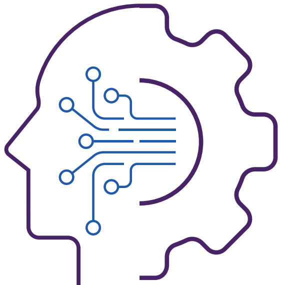


Additionally, nearly nine in ten SMBs (88%) believe their company's data is somewhat to much more secure when protected by AI/ML-enabled technology.

Based on these factors, we expect the adoption of AI/ML tools to increase within this space, though understanding of their uses and capabilities is likely to remain lower than that of larger organizations who can afford a greater number of IT security resources.

40 *"Does a company claiming to use artificial intelligence (AI) and machine learning (ML) to protect your data impact how you perceive the security of your data?"*





Key Takeaways for Small and Medium-Sized Businesses

SMBs agree: all businesses are vulnerable to cyberattacks.

That means it's critical to protect your business, even if you think you're unlikely to be targeted. In addition to your own security and cyber resilience practices, it's also important to vet the security of the vendors and partners in your supply chain. If someone else is holding your sensitive business data when they get breached, then your business is compromised too, even if you weren't the intended target.

If you don't have dedicated IT security resources, choose your solution providers wisely.

Many businesses don't have the resources to keep dedicated security experts on staff. Partner with vendors who use and provide AI/ML-enabled solutions, who share their security expertise or offer training, and who can advise you on the right products and product configurations for your unique environment and business needs.

Learn as much as you can about your tools to make the most of a limited budget.

Your cyber resilience strategy should be one of the most important items on your budget, but other costs sometimes have to take priority. If investing in a new solution lineup isn't feasible, we recommend investing instead in training your teams and end users to ensure you're getting the most out of the tools you already use.

CONSUMERS

Regional Highlights

United States

- Most likely to have been notified that their data had been stolen or breached
- Most likely to agree (87%), on some level, that all businesses are vulnerable to cyberattacks despite any protections in place

United Kingdom

- Most likely to say their financial data is extremely or very protected compared to the U.S., Australia/New Zealand, and Japan
- Nearly half believe their data is protected from all or most cyberattacks

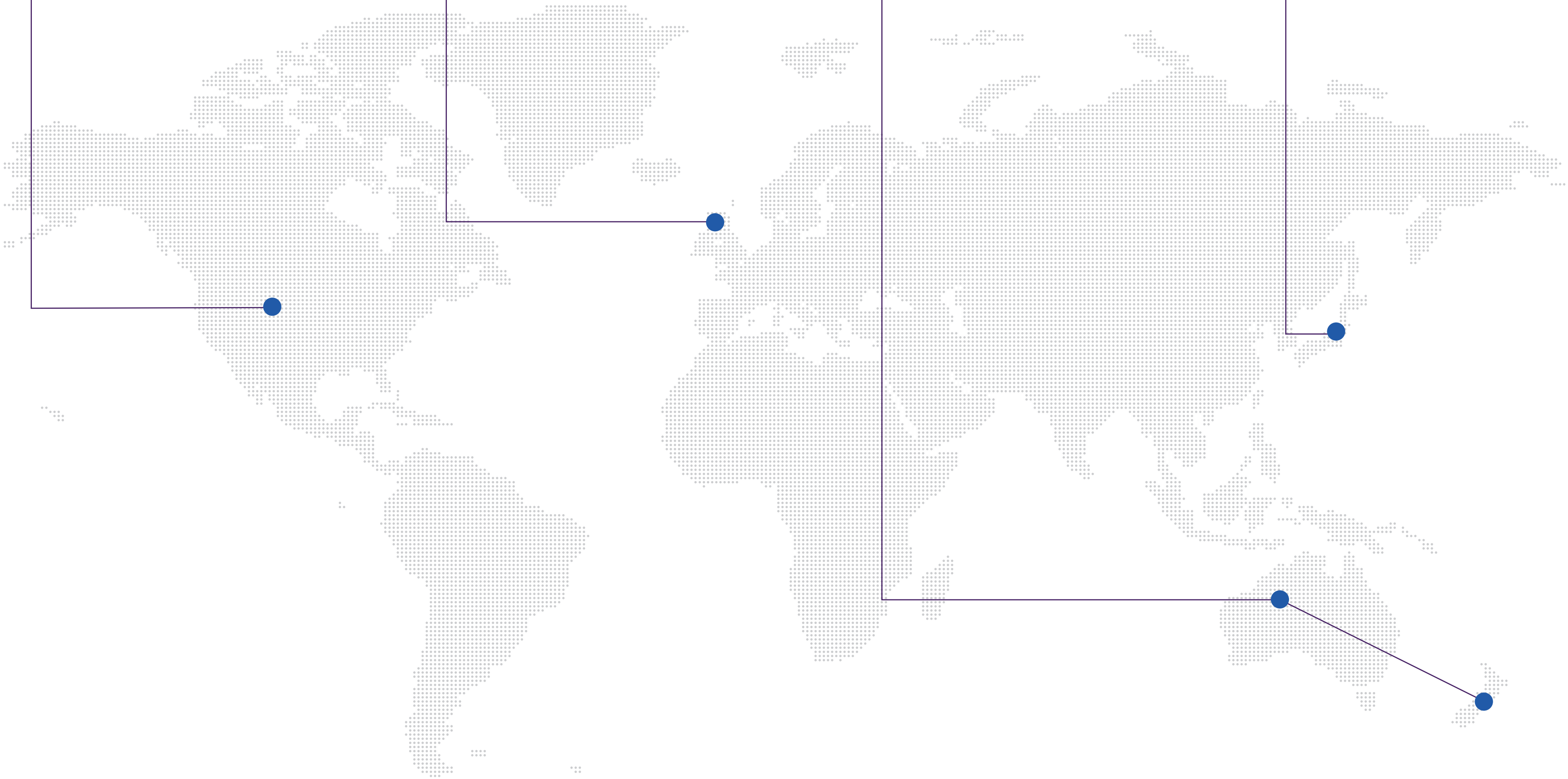
Australia/New Zealand

- Least likely to consider their health data to be extremely or very protected
- Least likely to claim any knowledge or understanding of AI/ML

Japan

Less likely to trust financial, healthcare and government organizations or companies to protect their data

Least likely to have been notified that their data had been stolen or breached

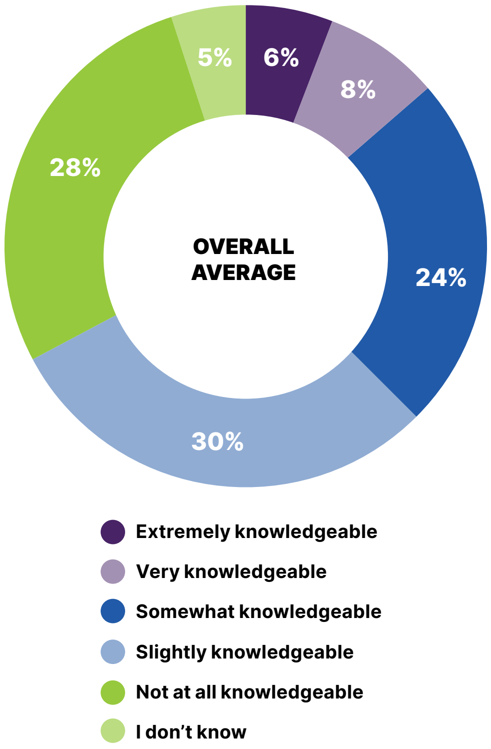


CURRENT OUTLOOK

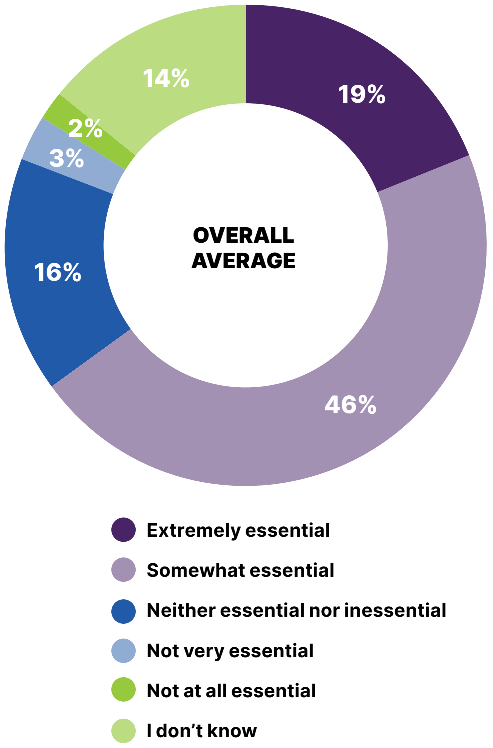
Of the audiences we surveyed, consumers were the least likely to express familiarity or comfort with AI and machine learning technologies and their role in cybersecurity. That's to be expected since home users are not IT decision-makers in the traditional sense. More than a quarter (28%) self-reported as "not at all knowledgeable" when it comes to AI/ML.

Despite their acknowledged gaps in understanding, two-thirds of respondents (65%) believe it's somewhat to extremely essential to use AI/ML to combat emerging cyber threats.

41 ***"How knowledgeable are you about artificial intelligence (AI) and machine learning (ML)?"***



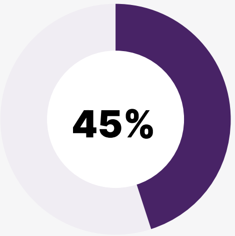
42 ***"How essential is the use of AI and machine learning in addressing current and future security threats?"***



When asked what cybersecurity precautions they take, consumers listed the following as their top three steps:

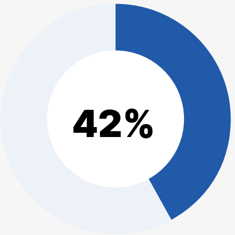
1

Using antivirus protection or antimalware protection on devices



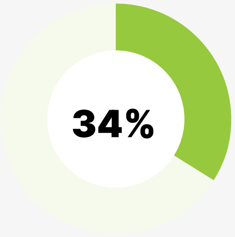
2

Installing software updates regularly

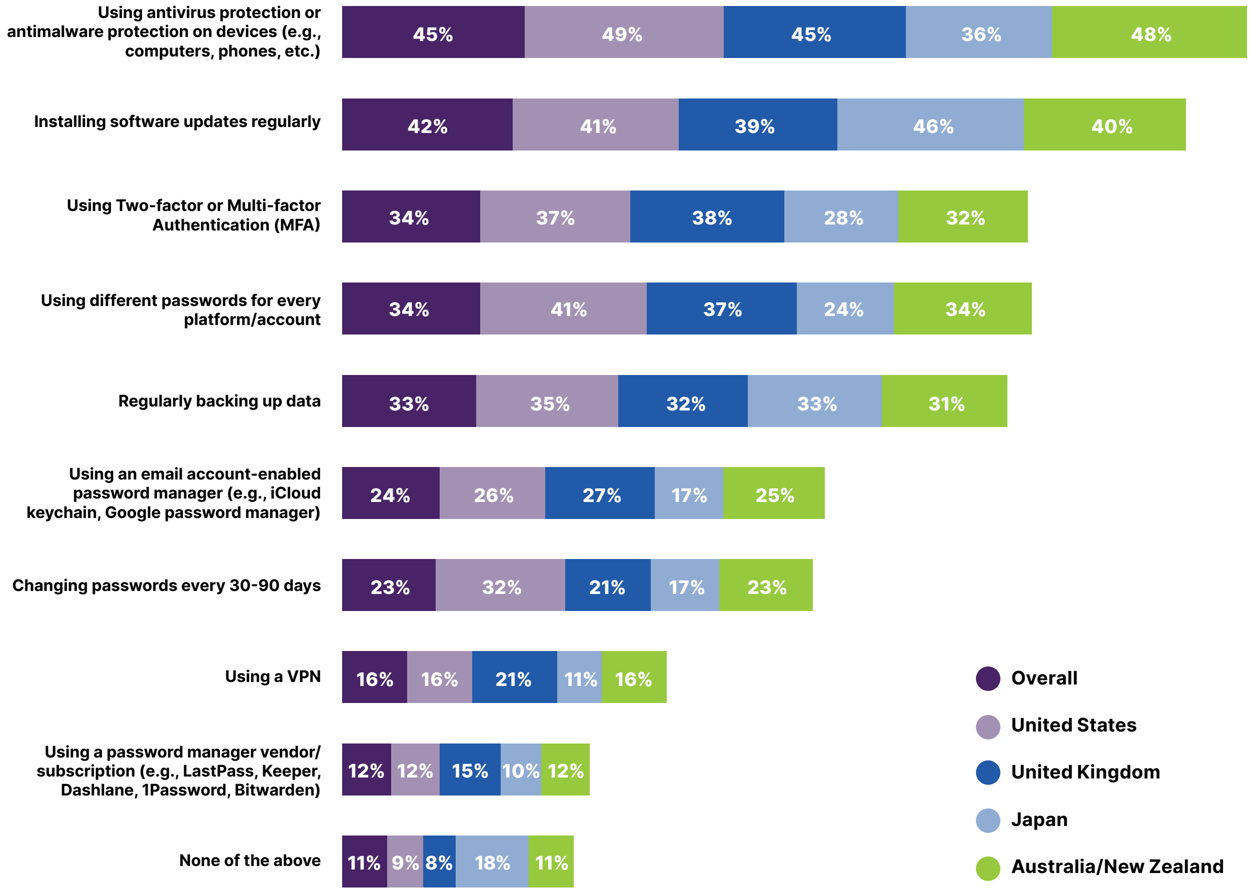


3

Using Two-factor or Multi-factor Authentication



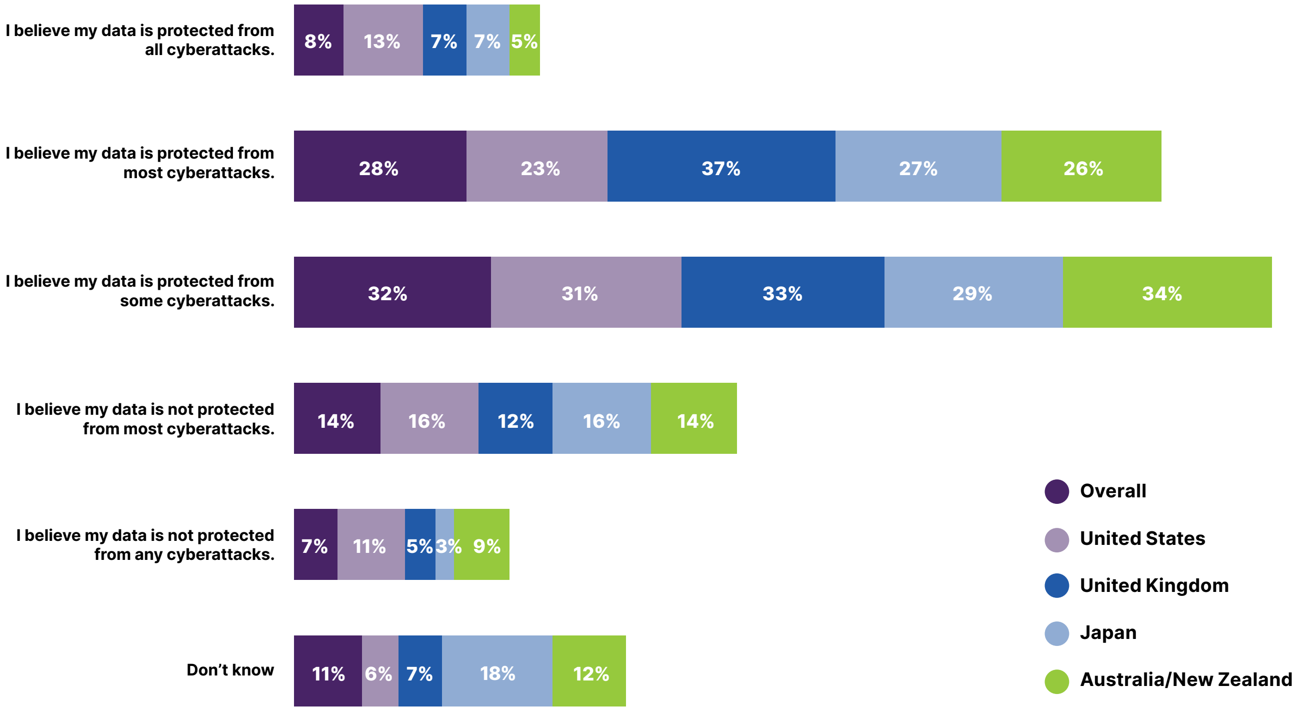
43 ***"Do you take any of the following cybersecurity precautions in your daily life?"***



11% of consumers don't take any cybersecurity precautions in their daily lives.

Despite whatever precautions consumers may take, about one-third of respondents (32%) believe their data is not protected enough, or simply don't know whether their data is safe, while 42% have personally experienced a data breach (see next section).

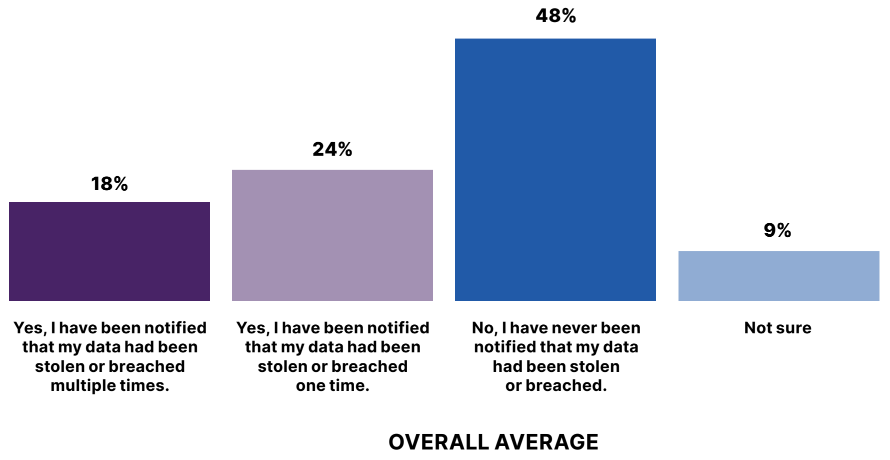
44 *"Do you believe that your data is protected from cyberattacks?"*



THE REALITY OF THE THREAT LANDSCAPE

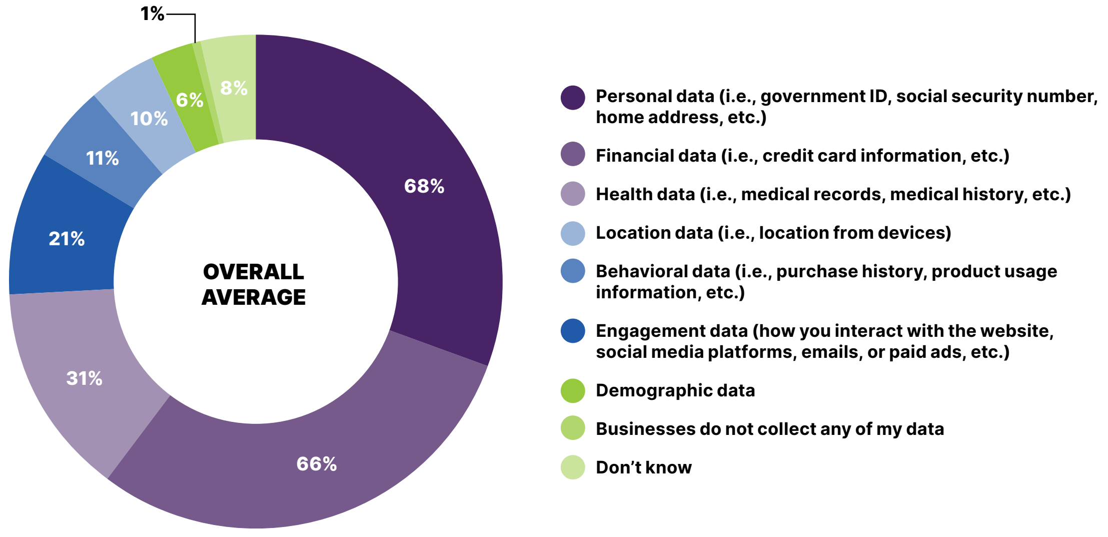
Two out of five (42%) consumers have been notified that their data has been stolen or breached at least once.

45 *"Have you ever been notified that your data had been stolen or breached?"*



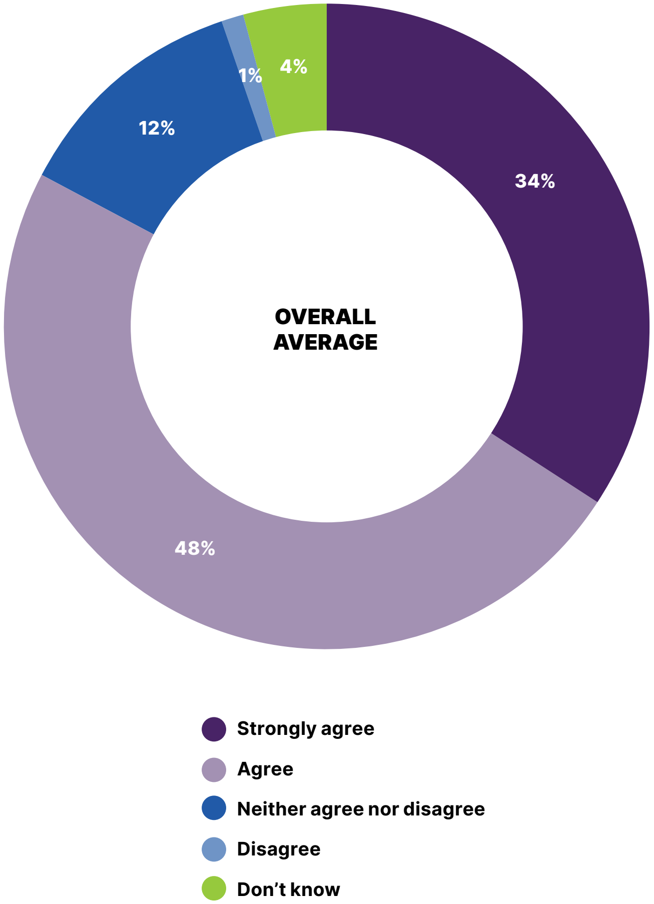
Although consumers reported a fairly high data breach percentage, they are extremely concerned with the protection of their data and won't trust just any company with it. In particular, personal data, financial data, and health data are their top priorities. More than one-third of consumers (38%) say they do not trust social media companies at all when it comes to protecting their data.

46 *"What types of your data are you most concerned about protecting?"*



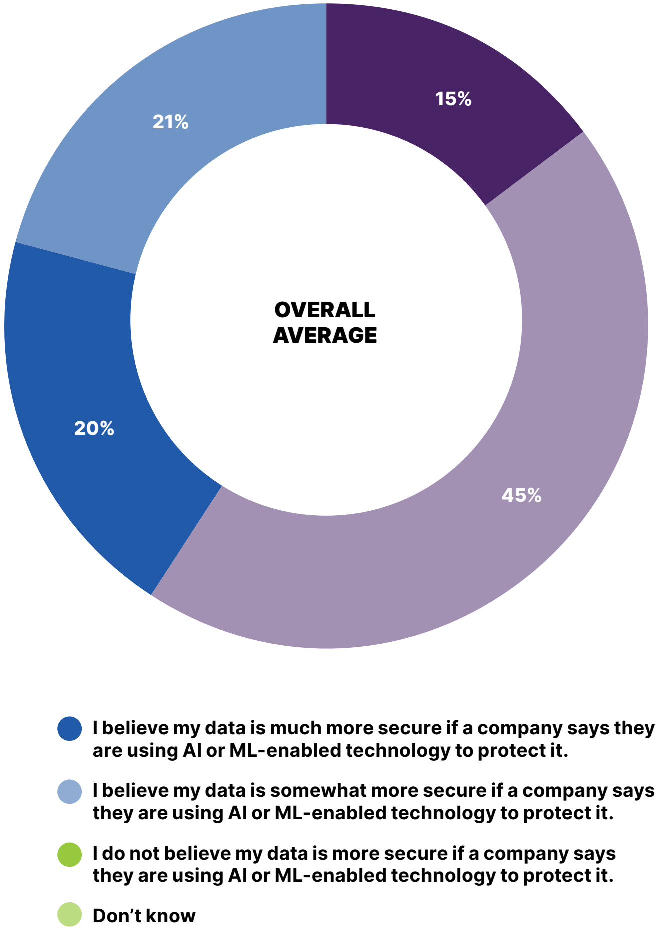
The level of trust in businesses and how they secure customer data aligns with consumers’ perceptions around business’ vulnerability to threats. Four out of five consumers (82%) agree or strongly agree that all businesses are vulnerable to cyberattacks at some level despite protections put in place.

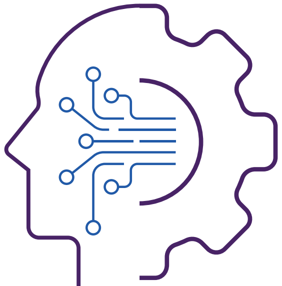
47 ***“Please indicate your level of agreement with the following statement: At some level, all businesses are vulnerable to cyberattacks despite any protections that may have been put in place.”***



And yet, even though consumers readily admitted a lack of familiarity with AI/ML, more than half of survey respondents (59%) believe their data is somewhat to much more secure if a company says they are using AI or ML-enabled technology to protect it.

48 ***“Does a company claiming to use artificial intelligence (AI) and machine learning (ML) to protect your data impact how you perceive the security of your data?”***





Key Takeaways for Consumers

All businesses are vulnerable to attacks. Be careful which ones have your data.

Consumers are right not to trust certain companies with their data. News reports about social media giants with improper data security practices, not to mention high-profile hacks on healthcare, financial, and government organizations, are pretty common. Always think twice before providing sensitive information and consider investing in identity protection and/or cyber insurance.

Less than half of consumers surveyed use antivirus, backup, or other security measures.

Even though most respondents claim to know better, only 45% of consumers are currently using an antivirus solution; 33% regularly back up their data; just 16% use a VPN; the list of less-than-ideal cyber-hygiene habits goes on. Any (reputable) security is better than none at all and is critical for keeping yourself, your family, and your important data safe from cyberattacks and data loss.

Security that uses AI/ML is better positioned to keep you safe. Do your research.

When picking your antivirus/antimalware, VPN, and backup solutions, try to look for the ones that use the latest technological advancements and cover all the different types of devices you use. That means you may have to do a little research into third party benchmarks and reviews. We recommend following a security-related news source, podcast, or blog to help you stay up to date. It can take some extra legwork but will keep you and your identity safer in the long run.

CONCLUSION

Although it's not necessary to fully understand a tool to reap the rewards of its use, it's clear IT decision-makers at enterprises and small and medium-sized businesses would benefit more from an increase in training and awareness. Despite some regional variance, there's still a fair amount of skepticism around the uses of AI/ML across all audiences surveyed, and many businesses and individuals seem to place more emphasis on whether they perceive their technology to be working, rather than concrete measures of its efficacy or whether they understand how it works.

With cyberattacks and other data threats on the rise, coupled with the complications of post-pandemic remote workforce needs, it's crucial that businesses and individuals alike embrace security and continuity layers equally; the key to maintaining resilience and service availability is a blend of proactive security and backup and disaster recovery solutions.

As businesses continue investing in these technologies throughout the rest of the year, they'll need to improve their understanding so they can invest more wisely in solutions that augment their existing resources. By choosing technology vendors who have long-standing experience, proven solutions, and demonstrated expertise in the areas where the organization or person in question needs guidance or service, businesses and individuals can further close the gaps in their security and continuity lineups – achieving ultimate resilience against attacks and data loss.

CARBONITE® + WEBROOT®

opentext™ Business Solutions

Methodology

This report is based on a survey conducted from March 26, 2021 through April 11, 2021 by LEWIS Research on behalf of OpenText and consisted of three online questionnaires, broken out by audience, of between 26 and 50 questions, requiring approximately 6-10 minutes or fewer to complete. The three audiences were 800 IT professionals at director-level or above who are the primary cybersecurity decision-makers at their organization of 1000 employees or more; 1,400 director-level or above professionals at SMBs with 250 employees or less; and 2,000 consumers (home users). This survey was conducted across four geographies: the United States, United Kingdom, Japan, and Australia/New Zealand.

About Carbonite + Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.

[1] Webroot. "Game Changers: AI and Machine Learning in Cybersecurity; a US/Japan Comparison." (December 2017)

[2] Webroot. "Knowledge Gaps: AI and Machine Learning in Cybersecurity." (January 2019)

[3] Webroot. "Smoke and Mirrors: Do AI and Machine Learning Make a Difference in Cybersecurity?" (February 2020)

[4] 55% refers to 33% who agree and 22% who strongly agree with the statement "I know some of our tools claim to use AI/ML, but I'm not sure what that means."

[5] 88% refers to 45% who agree and 43% who strongly agree with the statement "I understand and research the cybersecurity tools we use and specifically look for ones that use AI/ML to protect my organization."

[6] 60% refers to 27% who agree and 33% who strongly agree with the statement "I think cybersecurity tool vendors are being purposefully deceptive when it comes to how they market their AI/ML cybersecurity tools."