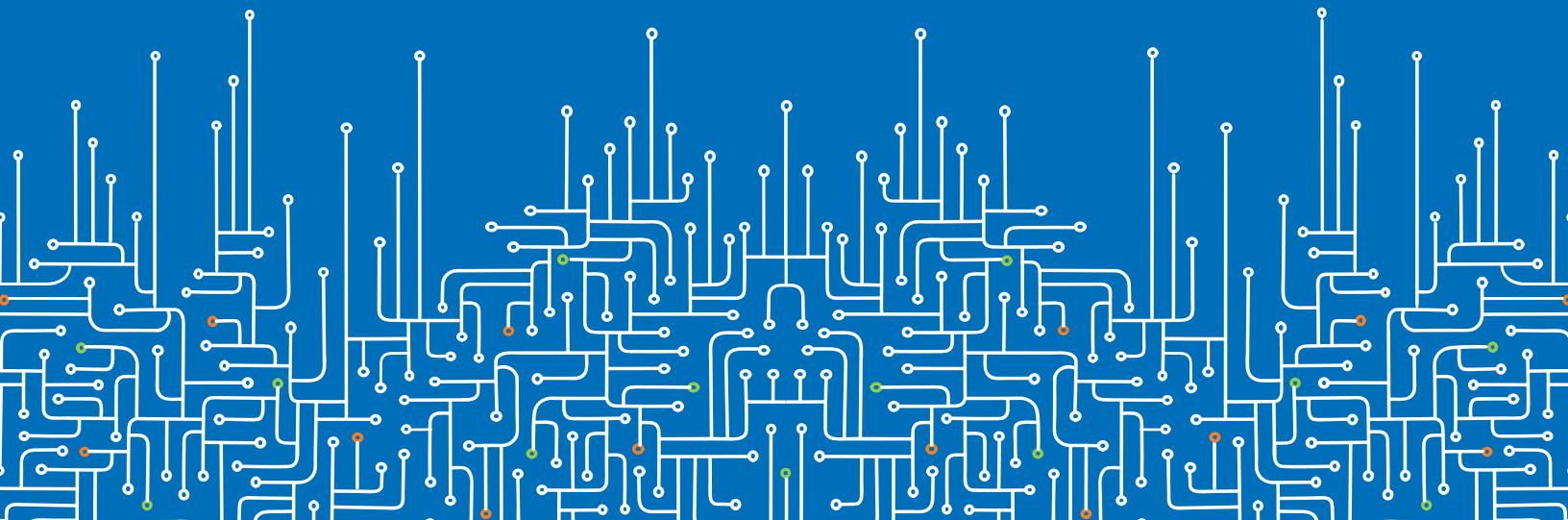
WEBROOT
Smarter Cybersecurity®

KNOWLEDGE GAPS: AI AND MACHINE LEARNING IN CYBERSECURITY

Perspectives from U.S. and Japanese IT Professionals



Executive Summary

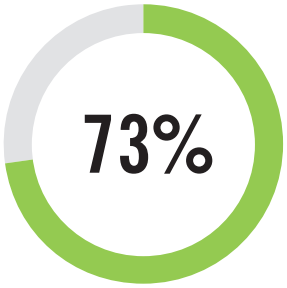
The use of artificial intelligence (AI) and machine learning (ML) in cybersecurity tools continues to grow. In 2017, we discovered that approximately 74% of businesses across the United States and Japan had already begun using some form of AI or ML to protect their organizations.[1] When we checked back in with organizations in both regions at the end of 2018, 73% of respondents we surveyed reported they plan to use even more AI/ML tools in 2019.

AIthough AI and ML cybersecurity tools are popular among IT professionals, many respondents claimed they don't fully understand the benefits of said tools. The overwhelming majority (72%) agree that, as long as their protection keeps them safe from cybercriminals, they do not care whether it uses AI or machine learning. And over half (58%) say that, while they know some of their tools use AI or ML, they're not entirely sure what that means. Further education on how these tools work and what value they bring would be beneficial to IT professionals across the globe, particularly since many plan to increase their cybersecurity spend in the coming months.

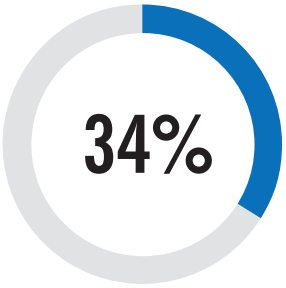
Interestingly, this survey revealed that IT professionals whose organizations experienced a damaging cybersecurity attack within the last 12 months have not lost faith in AI and ML tools. Additionally, 84% of respondents believe cybercriminals are also using AI and ML to in their attacks. When considered together, these two figures indicate a strong belief that AI/ML-based cybersecurity is no longer simply nice to have; it's crucial to stop modern cyberattacks.

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

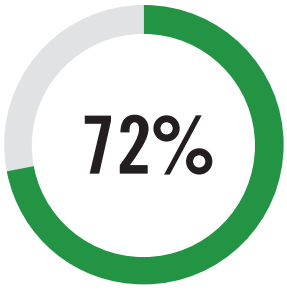
GLOBAL FINDINGS



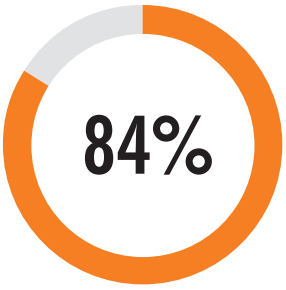
plan to use more AI/ML tools in 2019.



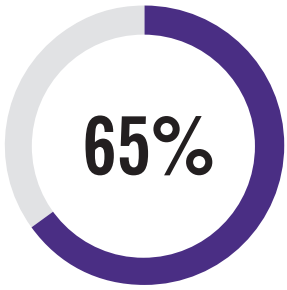
report their organization has experienced a damaging cyberattack in the last 12 months.



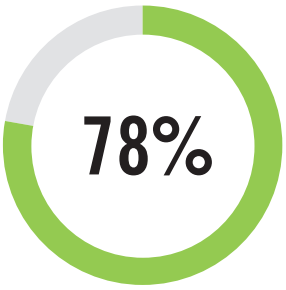
agree that as long as their protection keeps them safe from cybercriminals, they do not care if it uses AI/ML.



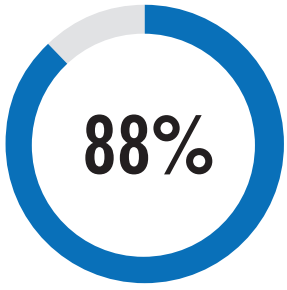
believe cybercriminals are using AI/ML to attack organizations.



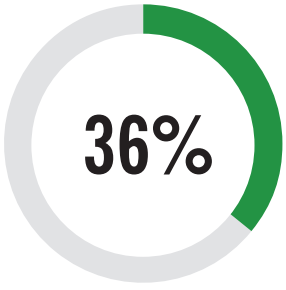
say it is very important that cybersecurity advertising mention use of AI/ML.



think their organization has everything it needs to defend against AI/ML-based cyberattacks.



report they understand how AI/ML is deployed in cybersecurity.



are completely certain where their cybersecurity vendors source their threat data.

The Current State of Cyberattacks on Businesses

The number of cyberattacks on businesses isn't dropping off. In fact, over one-third (34%) of survey respondents in the U.S. and Japan indicated their organizations had experienced a damaging security breach or attack within the last 12 months. What might come as a surprise is these attacks happened *despite* the organizations' increased spending on AI/ML-based cybersecurity tools, and a high level of confidence (76%) that their organization is safer because of their investment.

Response	Overall	US	Japan
Yes	34%	36%	32%
No	66%	64%	68%
Don't know	1%	1%	1%

Figure 1: "Has your organization experienced a damaging cybersecurity attack within the last 12 months, despite using AI/ML cybersecurity tools?"*

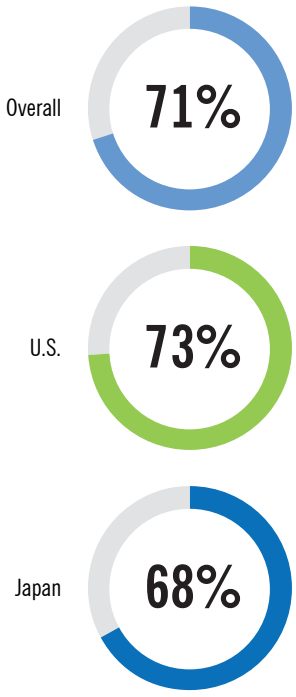


Figure 2: Number of organizations that spend more on AI/ML cybersecurity tools than they did two years ago

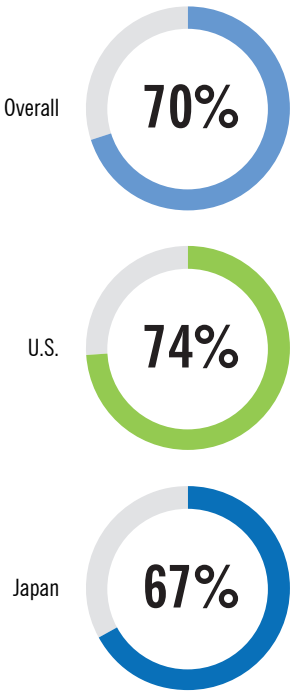


Figure 3: IT professionals who feel they spend enough to get all the tools needed to protect their organizations

** Percentages may not add up exactly due to rounding.*

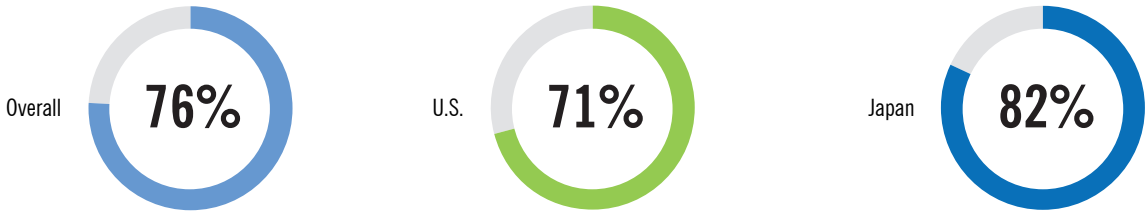


Figure 4: Respondents who believe using AI/ML-based cybersecurity makes their organizations safer

The Importance of AI and ML

Artificial intelligence and machine learning are hot topics, even "buzz words", in cybersecurity today, offering benefits that range from improved productivity and efficiency to faster threat detection and fewer false positives. But do individuals truly understand their complexity? When choosing a new cybersecurity tool, 35% of IT professionals consider AI or ML to be at least *somewhat important* in their decision-making process, and 65% consider these technologies a necessity. But, while 82% report a very or extremely high level of comfort with AI/ML, more than half (58%) are still not sure what it really means, and many don't know how their cybersecurity vendors source or update their threat data.

Response	Overall	US	Japan
Very Important	65%	70%	60%
Moderately Important	30%	25%	34%
Slightly Important	5%	4%	5%
Not Important	1%	1%	1%

Figure 5: "When choosing a new cybersecurity tool, is it important that it advertise its use of AI/ML?"*

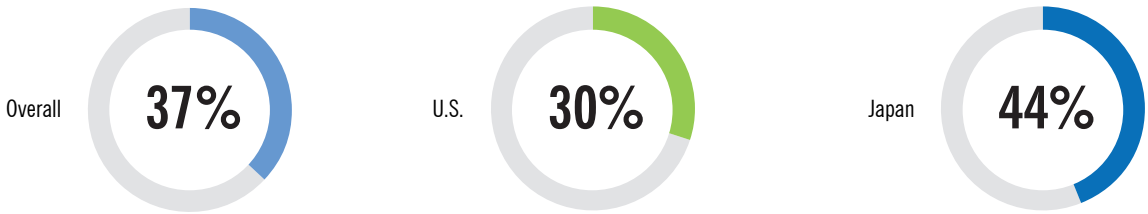


Figure 6: Respondents who feel their teams must fully understand a security solution before adopting it

** Percentages may not add up exactly due to rounding.*

Response	Overall	US	Japan
Extremely Comfortable	39%	49%	30%
Very comfortable	43%	42%	44%
Somewhat comfortable	13%	9%	17%
Not at all comfortable	6%	1%	11%

Figure 7: Self-reported level of comfort with AI/ML*

Response	Overall	US	Japan
Yes	71%	71%	70%
No	25%	26%	23%
Don't know	5%	3%	7%

Figure 8: "Do you know how often your cybersecurity vendor updates their AI/ML algorithms?"*

Response	Overall	US	Japan
I'm 100% certain where that threat data comes from.	36%	38%	33%
I'm fairly certain I know where the threat data comes from, but not 100% sure.	51%	51%	51%
I only know a little about where the threat data comes from.	9%	9%	10%
I have no idea where the threat data comes from.	5%	2%	7%

Figure 9: "Do you know where your cybersecurity vendor sources its threat data?"*

Response	Overall	US	Japan
Strongly agree	27%	28%	26%
Somewhat agree	32%	28%	35%
Neither agree nor disagree	20%	19%	21%
Somewhat disagree	11%	13%	9%
Strongly disagree	12%	14%	10%

Figure 10: "I know some of our tools say they use AI/ML, but I'm not sure what that means."*

** Percentages may not add up exactly due to rounding.*

Response	Overall	US	Japan
Strongly agree	34%	36%	31%
Somewhat agree	38%	40%	36%
Neither agree nor disagree	14%	11%	17%
Somewhat disagree	9%	9%	9%
Strongly disagree	6%	5%	8%

Figure 11: "As long as the tools we license help protect us against cybercriminals, I don't care if it uses AI/machine learning."*

The takeaways from the previous figures, especially Figure 11, are surprising. A full 72% of respondents are relatively indifferent to AI and ML as long as their organizations stay safe, yet, when it comes to advertising a new cybersecurity tool, most (65%) say it is very important that it mentions its use of AI or ML.

What the Future Holds

Cybersecurity budgets continue to increase, with 71% of today's organizations reporting they spend more on AI/ML than they did two years ago. Although the majority of IT professionals in the U.S. (74%) and Japan (67%) feel their organizations are spending enough to protect their businesses from cyberattacks, 26% and 28%, respectively, believe they could still be doing more.

Response	Overall	US	Japan
More	73%	71%	75%
About the same	25%	28%	23%
Fewer	0%	0%	1%
Don't know	2%	2%	2%

Figure 12: "Does your organization plan to use more or fewer AI/ML cybersecurity tools in 2019?"*

Response	Overall	US	Japan
Yes	81%	84%	78%
No	14%	12%	16%
Don't know	6%	5%	7%

Figure 13: "Do you believe your organization's current set of cybersecurity tools will help stop all cyber threats your organization faces?"*

** Percentages may not add up exactly due to rounding.*

Response	Overall	US	Japan
Yes	84%	86%	82%
No	8%	8%	8%
Don't know	8%	7%	10%

Figure 14: "Do you think cybercriminals use AI/ML tools to attack public and private organizations?"*

Response	Overall	US	Japan
Yes	78%	83%	72%
No	19%	14%	24%
Don't know	3%	3%	4%

Figure 15: Respondents who think their organization has everything it needs to successfully defend against AI/ML-based cyberattacks*

Response	Overall	US	Japan
Increased AI or machine learning adoption	47%	54%	41%
Training IT staff on new solutions	46%	53%	40%
New threat monitoring techniques/services	42%	43%	40%
Identifying and onboarding new technologies	39%	43%	35%
Training of general employees on compliance with internal cybersecurity rules	39%	43%	35%
Regulatory compliance (GDPR, HIPAA, etc.)	37%	41%	33%
Threat attribution	32%	34%	31%
Ransomware	30%	33%	28%
Nation state attacks	27%	21%	33%

Figure 16: "What are the biggest cybersecurity areas you plan to focus on in 2019?"*

** Percentages may not add up exactly due to rounding.*

Conclusion

This year's survey yielded a number of surprising results. While IT professionals in the U.S. reported significantly higher levels of comfort using artificial intelligence and machine learning technology than their Japanese counterparts (91% and 74%, respectively), both groups expressed a nearly equal amount of uncertainty around what AI/ML means in terms of the tools they use. Japanese respondents placed more importance on fully understanding tools before they implement them, while their American peers attached greater significance to cybersecurity vendors mentioning their use of AI or ML in advertising.

It's clear there are knowledge gaps around how artificial intelligence and machine learning tools work to secure businesses and streamline operations. With the majority of respondents planning to increase spending on AI/ML technologies in 2019, businesses will need to improve their understanding of these tools to see maximum value. Partnering with cybersecurity vendors who have long-standing experience using and developing AI/ML, and who can provide expert guidance, will help businesses achieve the highest levels of security and efficiency possible—without draining resources.

Methodology

Survey respondents were provided by Branded Research Inc., which has an active proprietary global panel of over 2 million respondents. The survey was conducted by LEWIS between November 26 and December 5, 2018, and consisted of an online survey of 37 questions total, requiring approximately 10 minutes. For all survey respondents, LEWIS partners with Imperium to only work with companies who implement their quality control services on their sampling services. Imperium is solely focused on helping companies guarantee data integrity and comply with industry regulations. Survey responses were received from 400 full-time IT professionals at the IT director level and above; 200 of which were from the United States, and 200 from Japan. Respondents represented organizations that had 250 employees or more, and 87% were the primary decision makers for cybersecurity tools purchased within their organization. The overall margin of error was 5% at a 95% confidence interval.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com