SECTOR IN-DEPTH
22 January 2026

Send Your Feedback

TABLE OF CONTENTS

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

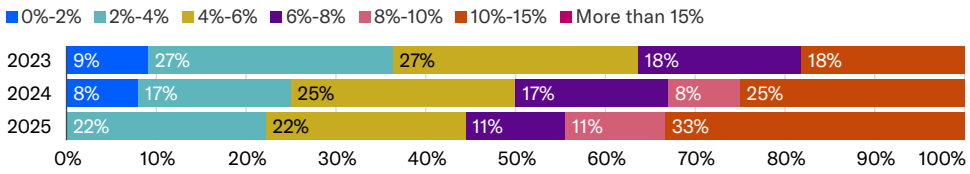
Automotive – Global

Cybersecurity – Auto sector performs well, continued diligence needed as attacks rise

Cyber risk within the automotive sector — which includes carmakers and auto parts suppliers — is accelerating as the connected car experience creates vulnerabilities. Increasing digitalization, software-based functions (like infotainment, advanced driver assistance, autonomous driving) and a surge in the use of artificial intelligence leave the industry susceptible to security breaches. Beyond exposure to ransomware attacks that can disrupt production and other key activities, auto manufacturers also face the potential for consumer data and privacy breaches at their captive finance operations. The risk of manipulation of remote vehicle access, safety and operations (braking, acceleration) pose potentially more severe consequences. With high efficiency-driven manufacturing environments, complex supply chains and importance to regional economies, the automotive industry is a prime target for cybercriminals. The sector continues to invest in cyber defense, dedicating larger portions of budgets to cybersecurity (see Exhibit 1) and maintaining high levels of standalone cyber insurance. This may prove important since we expect cyber risk will shift into higher gear this year as attackers exploit increasingly effective AI tools to enhance their tactics.

Nearly 80% of the automotive sector respondents to our survey have a specific, focused role of Chief Information Security Officer (CISO). CISOs are specialized experts responsible for protecting IT systems and data by overseeing cybersecurity, risk management and compliance. This differs from Chief Information Officers (CIO), who more broadly focus on managing and optimizing an organization's IT strategy, system and technology. This survey also highlights a growing trend for cybersecurity managers to report directly to senior management. C-suite access improves the cyber manager's ability to raise awareness and promote strategic alignment between cybersecurity practices and core business objectives, often translating into more resources for cyber defense and preparedness.

Exhibit 1
Cyber spending is on the rise
Share of the respondent's total technology budget allocated to cybersecurity



Source: Moody's Ratings

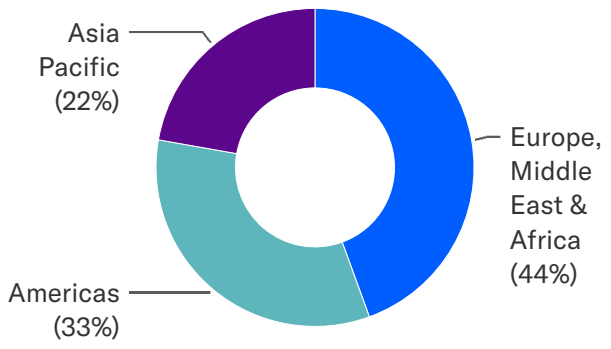
Moody's cyber survey in focus

Our 2025 Cyber Survey was a 60-question evaluation of cybersecurity practices among global debt issuers. The survey provides valuable insights into a growing risk that has the potential to significantly affect the credit metrics of all of our rated issuers. Companies and organizations with high debt and low liquidity are particularly vulnerable to the substantial costs that can follow a cyberattack, but the increasing frequency and sophistication of these attacks pose significant financial, reputational and legal risks to all issuers. There have been 28 credit rating actions so far directly linked to cyber incidents.

Survey metrics:

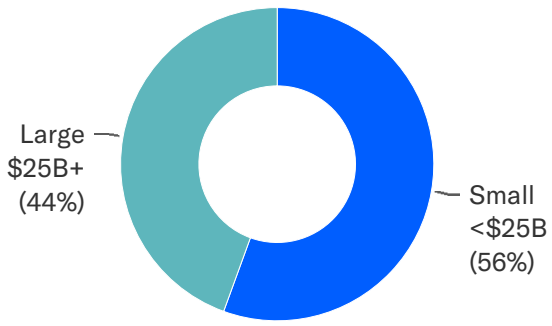
- This is our third global cybersecurity survey
- We received nearly 2,000 responses globally with 18 from the global automotive sector
  - Five from automobile manufacturers and 13 from automotive suppliers
- Automobile manufacturers and automotive suppliers were both categorized as "High Risk" sectors in our 2024 global cyber heat map, elevated from "Moderate Risk" in our 2022 heat map

Exhibit 2
EMEA led in cyber survey respondents
Percent of automotive survey respondents by region



Source: Moody's Ratings

Exhibit 3
Most respondents were smaller companies
Percent of automotive survey respondents by revenue size



Source: Moody's Ratings

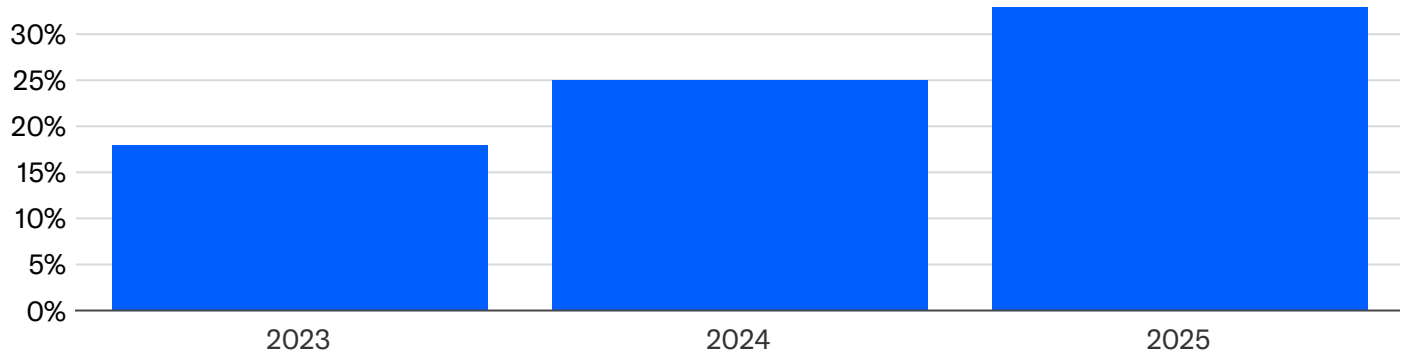
Cyber budgets rising largely in-line with global standards though cyber personnel not expected to expand

The automotive sector is allocating a growing share of its technology budgets to cybersecurity (see Exhibit 4), supporting the rising importance of cybersecurity protections. Within our rated universe as of December 2025, the automotive sector had the highest percentage of issuers that experienced a cyber incident within the last 24 months. More specifically, since the June 2024 cyberattack against CDK Global (B3 negative), a management software provider for auto dealerships, there have been several higher profile, very disruptive attacks on the industry. Separate customer data breaches at third-party vendors affecting Stellantis N.V. (Baa2 negative) in September 2025 and Renault UK (Renault S.A. - Ba1 positive) in October 2025 highlight vulnerabilities in the industry's supply chain. Automaker Jaguar Land Rover Automotive Plc (JLR - Ba1 negative) suffered a cyberattack in August 2025, resulting in a complete shutdown of its systems and major disruption to its sales and production capabilities. The attack illustrated the ripple effect on international supply chains, third-party vendors and regional economies as the UK government stepped in with a loan guarantee worth £1.5 billion. In response, we changed the rating outlook to negative in September 2025, to reflect the damage to JLR's credit metrics and uncertain time frame for JLR to fully recover. The increase in frequency and severity in attacks is raising the stakes in cybersecurity defense.

Exhibit 4

Automotive sector continues to boost percentage of technology budgets for cybersecurity

Percent of survey respondents allocating more than 10% of IT budgets to cybersecurity



Source: Moody's Ratings

» Every sector respondent has a multiyear road map or strategy for managing cyber risk which is supported by the fact that nearly 90% of respondents have a separate line item within their budgets for cybersecurity

» Only 25% of respondents indicated intentions to increase cybersecurity staffing (in-house and/or outsourced) over the next 12 months, below the global survey score of 40%

» However, 13% of sector respondents expect to decrease cyber personnel, which contradicts other sectors; this could be a result of AI-enabled technologies assuming some cyber defense tasks/functions

» Less than 20% of the respondents indicated that 100% of the cyber staff are full-time employees, highlighting greater reliance on outsourcing compared to the global rate of 40%; Asia-Pacific showed higher use of external cyber expertise, which can be flexible and more cost-effective

Supply chain vulnerabilities remain a primary concern for automotive sector

Automotive companies may implement robust cybersecurity measures, but as seen with several of the 2025 cyberattacks on the industry, vendors and suppliers often do not adhere to the same standards. Even as internal cyber defenses improve for rated companies, attackers are also looking for vulnerabilities in the supply chain to bypass these stronger protections and expose companies' systems and data.

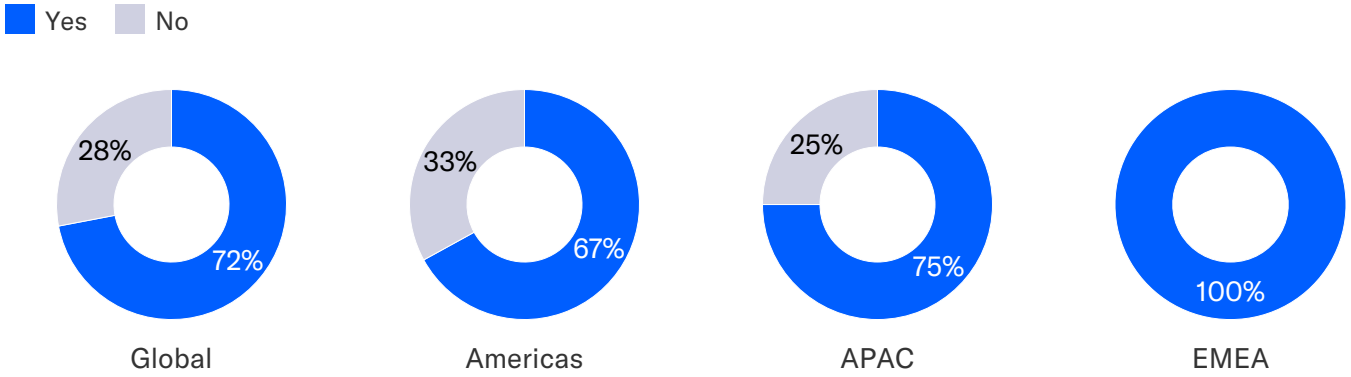
» Most of the respondents maintain a third-party vendor cyber risk program with EMEA especially strong in this area (see Exhibit 5)

» Frequency of reviewing vendors' cybersecurity risk practices lags for the automotive suppliers compared with the automobile manufacturers and global sector standards (see Exhibit 6)

» EMEA is an outlier when it comes to not requiring vendors (software providers and others) with access to issuers' IT systems to carry cyber insurance

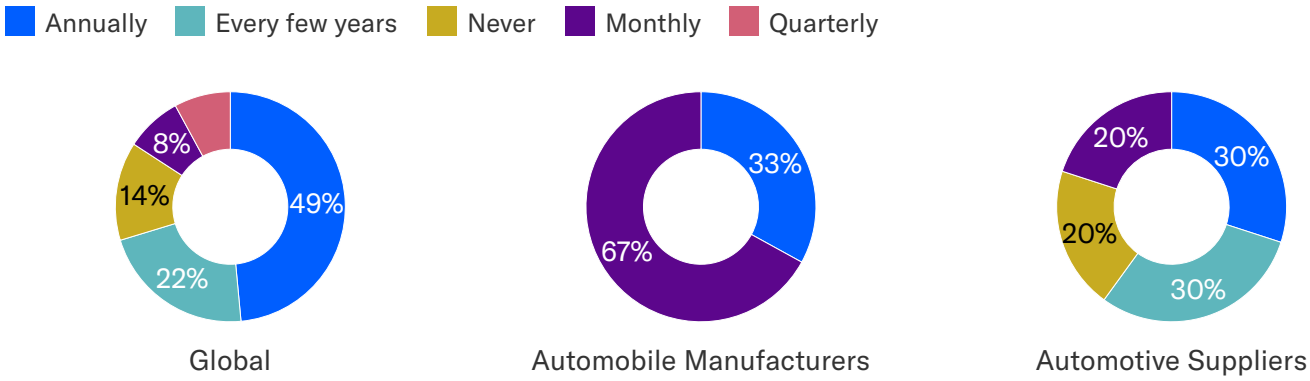
» Nearly 80% of sector respondents require a cybersecurity assessment of a target company before completing an M&A transaction, considerably higher than the global rate of just over 40% (see Exhibit 7)

Exhibit 5
All EMEA respondents demand vendors have cyber risk programs
Does the issuer maintain a third-party vendor cyber risk program?



Source: Moody's Ratings

Exhibit 6
Auto manufacturers the most diligent in reviewing vendors' cybersecurity
How frequently are vendors' cybersecurity risk practices reviewed?



Source: Moody's Ratings

Exhibit 7
Third-party risk management practices vary broadly by region

	Global	Americas	Asia Pacific	Europe, Middle East & Africa
Require vendors to carry cyber insurance in most or all cases	44%	40%	33%	0%
Maintain a Service Level Agreement addressing cyber breaches with critical vendors	84%	83%	100%	100%
Require a cybersecurity assessment of a target company prior to completing an M&A transaction	43%	67%	100%	80%

Source: Moody's Ratings

Standalone cyber insurance widely adopted across sector, use of key cyber controls uneven

Cyber insurance is a common tool for organizations to manage cyber risk exposure, despite rising premiums over the past few years. Since our first cyber survey, the automotive sector has maintained a high adoption rate of standalone cyber insurance with global cyber insurance adoption gradually increasing the last couple of years.

» Cyber insurance coverage within the automotive sector is higher (92%) than the global score of 80%

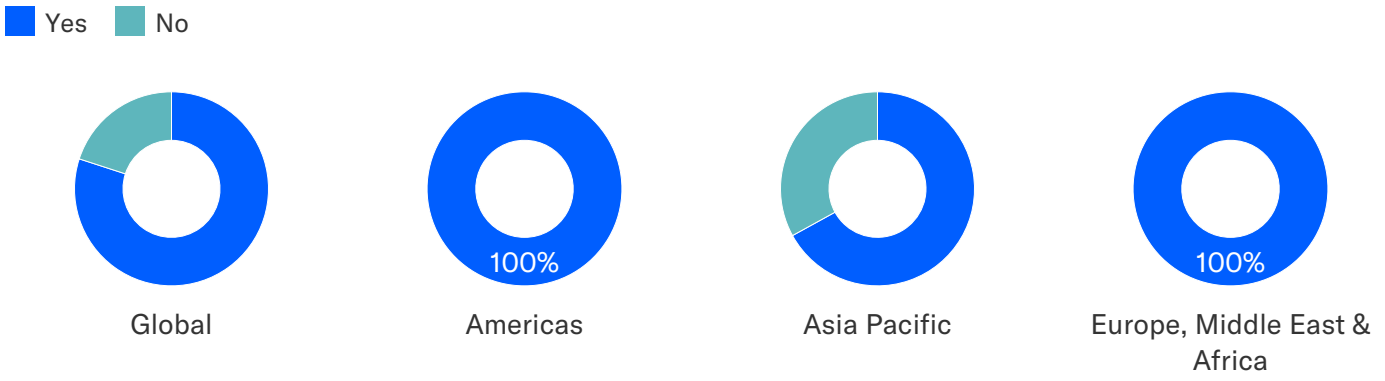
» APAC lags the Americas and EMEA in carrying cyber insurance (see Exhibit 8), but this essentially reflects limited availability of insurance outside of North America

» Similarly, cyber insurance policies in APAC do not include system failure coverage[1], versus 100% system failure coverage in EMEA and 60% in the Americas

» All respondents expect to buy the same amount of standalone cyber insurance in 2025

Exhibit 8

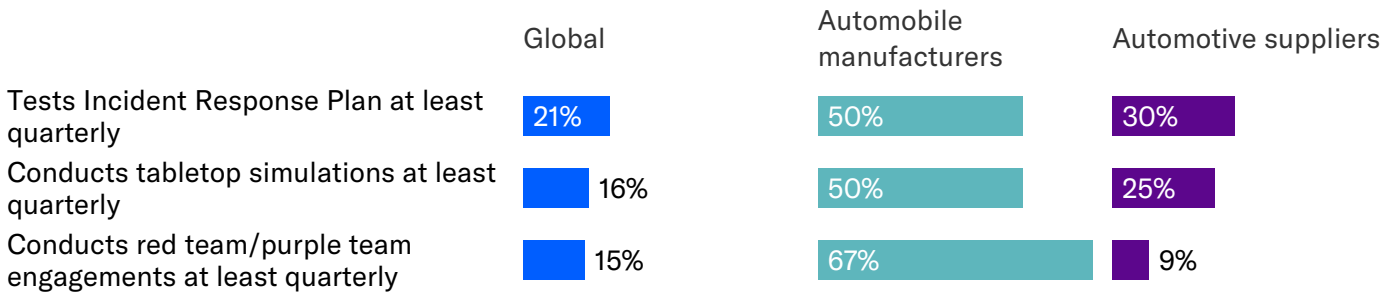
Automotive sector maintains a high adoption rate of standalone cyber insurance



Source: Moody's Ratings

The automotive sector continues to compare favorably to other sectors when it comes to how frequently it tests basic, foundational cyber defenses. Over one-third of respondents conduct at least quarterly testing of incident response plans. In addition, more sophisticated and costly tabletop simulations within the sector are conducted more often (see Exhibit 9) than the global average. More complex cyber defense practices such as red team/purple team engagements are conducted at a similar rate as global standards.

Exhibit 9
Auto manufacturers outpace auto parts suppliers in regular cyber testing, incident response planning



Source: Moody's Ratings

Still, respondents show mixed results on other common cyber hygiene practices and exercises, highlighting some gaps that will need to be addressed over time.

» Nearly 80% of the respondents have a program for responding to external reports of security issues affecting the issuer's products or operations versus only 55% globally

» The sector does a good job of backing up data and/or systems, with respondents backing up information daily (77%) or at least weekly (23%), however the sector was shy of global standards in scanning backup data for malware or other vulnerabilities

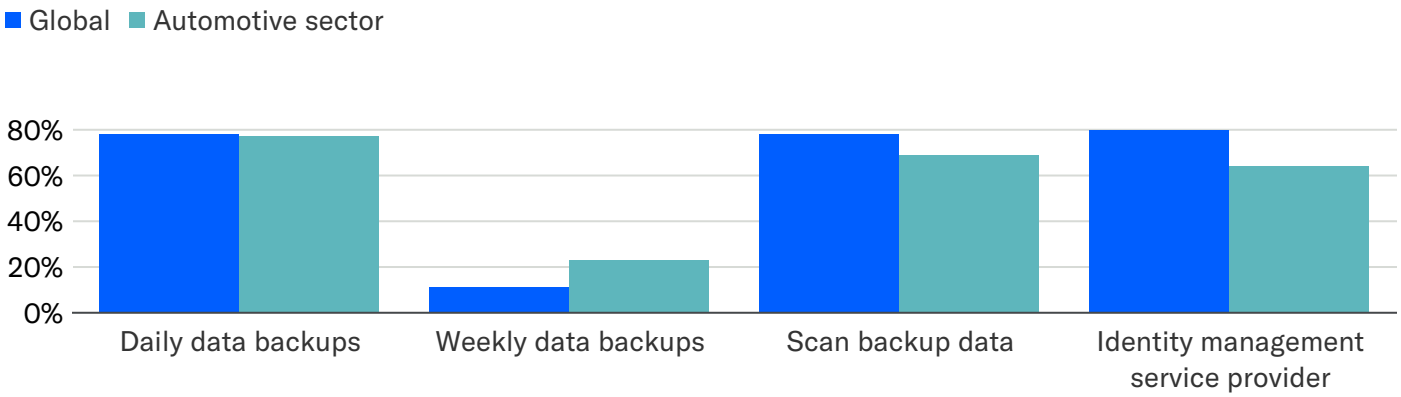
» Less than two-thirds of the sector uses an identity management service provider, compared to 80% globally, highlighting a gap in authenticating digital identities and simplifying access control (see Exhibit 10)

» The sector modestly exceeds the global score in use of multi-factor authentication (MFA)

» The auto sector also excels in managing and assessing End-of-Life software risk which enables timely upgrades/replacements while minimizing system disruptions and vulnerabilities

» Nearly two-thirds of respondents maintain a program that determines where open-source software (OSS) is used and embedded with 100% of these respondents having the ability to review and approve the source code; this helps preserve safe technological innovation despite the decentralized nature of OSS

Exhibit 10
Lower adoption rates of common cyber hygiene practices within auto sector



Source: Moody's Ratings

AI governance practices exceed global use standards, reflect prudent implementation and controls

AI technologies, including machine learning, predictive analytics and generative AI (GenAI) are becoming integral to automotive industry operations. While AI enhances cyber defenses and risk management, it also introduces new risks and complexities, including potential leaks of sensitive data via public AI platforms.

» Public AI tools like OpenAI's ChatGPT or Google's Gemini often process data on external servers. This means that submitting proprietary information could expose sensitive data, potentially violating internal data-handling policies or confidentiality agreements, or leading to unintentional leaks

» The auto sector is actively addressing the need for AI controls within their cybersecurity strategies, with 87% of respondents maintaining a formal policy governing the use of AI tools (see Exhibit 11)

  – This compares favorably to the global score of around 70%

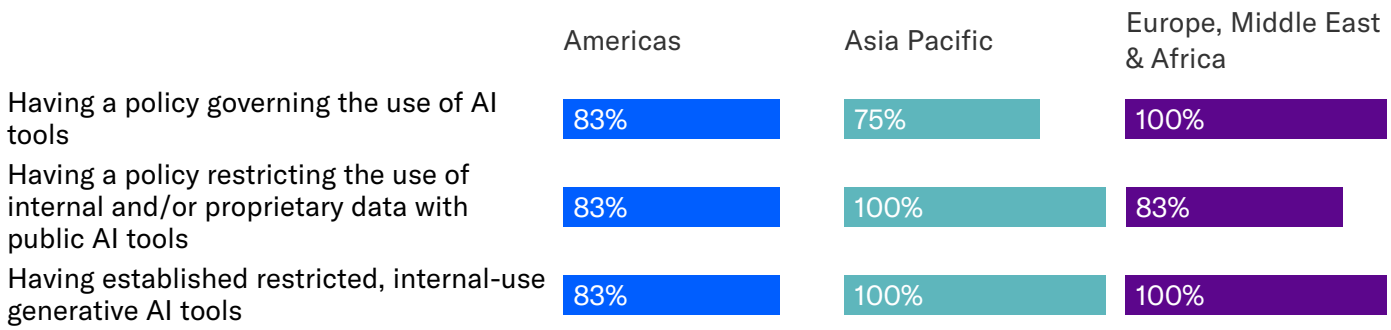
  – EMEA leads in this initiative

» All of APAC respondents follow the Open Worldwide Application Security Project (OWASP) Top 10 for use of GenAI, while none of the Americas respondents use it

  – OWASP is widely recognized as a standard for identifying and prioritizing application security risks, making it a trusted reference for secure development practices

Exhibit 11

Implementation of AI-related governance policies is high, especially in EMEA



Source: Moody's Ratings

Appendix

Exhibit 12

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
Number of responses	1,952	705	18	6	4	8	5	13	8	10	8	10
GOVERNANCE												
What is the title of the issuer's most senior employee (i.e. senior cybersecurity manager) whose primary responsibility is cybersecurity?												
Chief Information Officer	14%	15%	6%	0%		13%	0%	8%	13%	0%	13%	0%
Chief Information Security Officer	44%	49%	78%	67%		75%	80%	77%	75%	80%	50%	100%
Other	39%	35%	17%	33%		13%	20%	15%	13%	20%	38%	0%
N/a, the issuer does not have an employee responsible for cybersecurity	3%	1%										
To whom does the senior cybersecurity manager report?												
Chief Executive Officer/Chief Financial Officer	28%	27%	28%	17%		25%	20%	31%	25%	30%	38%	20%
Chief Information Officer/Chief Security Officer	35%	38%	67%	83%		63%	60%	69%	63%	70%	50%	80%
Chief Technology Officer	12%	14%										
Other	26%	22%	6%	0%		13%	20%	0%	13%	0%	13%	0%
How many times per year does the issuer's chief executive receive direct briefings from the senior cybersecurity manager?												
At least monthly	41%	34%	25%	0%		50%	75%	8%	67%	0%	0%	40%
At least quarterly, but less than once per month	35%	43%	38%	67%		17%	0%	50%	17%	50%	50%	30%
At least semi-annually, but less than once per quarter	11%	11%	25%	0%		33%	25%	25%	17%	30%	33%	20%
At least yearly, but less than semi-annually	8%	9%	13%	33%		0%	0%	17%	0%	20%	17%	10%
Every few years	1%	1%										
Never	3%	2%										
Does compensation for the issuer's chief executive depend on meeting defined cybersecurity performance objectives?												
Yes	21%	23%	36%	20%		25%	75%	14%	75%	14%	17%	60%
No	79%	77%	64%	80%		75%	25%	86%	25%	86%	83%	40%
How many times per year does the issuer's Board of Directors receive briefings from the senior cybersecurity manager?												
At least monthly	6%	4%	7%	0%		17%	0%	10%	20%	0%	14%	0%
At least quarterly, but less than once per month	35%	46%	43%	33%		33%	75%	30%	60%	33%	29%	57%
At least semi-annually, but less than once per quarter	17%	18%	21%	33%		17%	0%	30%	0%	33%	29%	14%
At least yearly, but less than semi-annually	27%	22%	29%	33%		33%	25%	30%	20%	33%	29%	29%
Every few years	5%	3%										
Never	9%	7%										
Does the issuer's Board of Directors have a dedicated cybersecurity committee?												
Yes	23%	25%	41%	0%		71%	75%	31%	71%	20%	29%	50%
No	77%	75%	59%	100%		29%	25%	69%	29%	80%	71%	50%
Do any of the issuer's Board Directors have current or past experience leading a cybersecurity team?												
Yes	32%	39%	58%	50%		50%	50%	60%	80%	43%	33%	83%
No	68%	61%	42%	50%		50%	50%	40%	20%	57%	67%	17%
Does the issuer have a multi-year roadmap or strategy for managing cyber risk?												
Yes	89%	93%	100%	100%		100%	100%	100%	100%	100%	100%	100%
No	11%	7%										
Does the issuer assess cyber risk in terms of financial impact (often called "cyber risk quantification")?												
Yes	69%	73%	75%	67%		86%	67%	77%	83%	70%	57%	89%
No	31%	27%	25%	33%		14%	33%	23%	17%	30%	43%	11%
Does the issuer use the results of the cyber risk quantification assessment to inform and take action on its cyber risk management plan?												
Yes	77%	81%	88%	100%		86%	75%	92%	86%	89%	83%	90%
No	23%	19%	13%	0%		14%	25%	8%	14%	11%	17%	10%

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
OPERATIONS												
Is cyber risk centrally managed across the issuer's subsidiaries, or managed separately at each subsidiary?												
Centrally managed	90%	91%	81%	100%		71%	67%	85%	50%	100%	100%	67%
Separately managed	10%	9%	19%	0%		29%	33%	15%	50%	0%	0%	33%
Over the next twelve months, does the issuer expect the total number of cyber employees (in-house and/or outsourced) to increase, decrease, or stay the same?												
Increase	40%	44%	25%	17%		0%	25%	25%	33%	20%	14%	33%
Decrease	1%	2%	13%	0%		33%	25%	8%	17%	10%	0%	22%
Stay the same	52%	46%	50%	83%		50%	25%	58%	17%	70%	71%	33%
I don't know	7%	8%	13%	0%		17%	25%	8%	33%	0%	14%	11%
What percentage of current cyber employees are outsourced?												
0%	40%	29%	18%	17%		0%	0%	22%	0%	22%	17%	20%
1%-10%	18%	21%	18%	17%		33%	0%	22%	0%	22%	17%	20%
10%-25%	15%	16%	18%	17%		33%	50%	11%	50%	11%	0%	40%
25%-50%	12%	15%	27%	33%		0%	50%	22%	50%	22%	33%	20%
50%-75%	7%	12%	18%	17%		33%	0%	22%	0%	22%	33%	0%
75%-100%	7%	7%										
Does cybersecurity have its own line item in the issuer's budgetary process?												
Yes	69%	76%	88%	67%		100%	100%	85%	100%	80%	71%	100%
No	31%	24%	13%	33%		0%	0%	15%	0%	20%	29%	0%
What percentage of the issuer's total technology budget was allocated to cybersecurity in 2023?												
0%-2%	13%	11%	9%	17%		0%	0%	10%	0%	11%	0%	20%
2%-4%	14%	18%	27%	33%		0%	0%	30%	0%	33%	33%	20%
4%-6%	20%	22%	27%	17%		50%	100%	20%	50%	22%	33%	20%
6%-8%	15%	15%	18%	0%		50%	0%	20%	50%	11%	17%	20%
8%-10%	15%	14%										
10%-15%	13%	12%	18%	33%		0%	0%	20%	0%	22%	17%	20%
More than 15%	10%	8%										
What percentage of the issuer's total technology budget was allocated to cybersecurity in 2024?												
0%-2%	8%	6%	8%	17%		0%	0%	9%	0%	10%	0%	17%
2%-4%	13%	15%	17%	17%		0%	0%	18%	0%	20%	17%	17%
4%-6%	20%	21%	25%	17%		33%	100%	18%	50%	20%	33%	17%
6%-8%	15%	19%	17%	17%		0%	0%	18%	50%	10%	17%	17%
8%-10%	17%	15%	8%	0%		33%	0%	9%	0%	10%	17%	0%
10%-15%	15%	15%	25%	33%		33%	0%	27%	0%	30%	17%	33%
More than 15%	11%	9%										
What percentage of the issuer's total technology budget is allocated to cybersecurity in 2025?												
0%-2%	7%	4%										
2%-4%	11%	12%	22%	33%		0%	0%	22%	0%	22%	17%	33%
4%-6%	18%	20%	22%	17%		33%	0%	22%	0%	22%	33%	0%
6%-8%	16%	19%	11%	17%		0%	0%	11%	0%	11%	17%	0%
8%-10%	18%	18%	11%	0%		33%	0%	11%	0%	11%	17%	0%
10%-15%	17%	16%	33%	33%		33%	0%	33%	0%	33%	17%	67%

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
What is the total percentage change in the amount spent on cybersecurity between 2020 and 2024?												
Less than -25%	4%	2%										
-25%-0%	2%	2%										
0%-25%	46%	38%	27%	17%		67%	50%	22%	33%	25%	17%	40%
25%-50%	18%	22%	45%	50%		33%	0%	56%	33%	50%	67%	20%
50%-75%	10%	11%	18%	17%		0%	50%	11%	33%	13%	17%	20%
75%-100%	6%	9%	9%	17%		0%	0%	11%	0%	13%	0%	20%
More than 100%	14%	17%										
How often does the issuer engage with or educate personnel on cyber issues?												
Monthly or more	55%	58%	63%	67%		50%	50%	67%	67%	60%	83%	50%
Quarterly	24%	27%	25%	17%		33%	25%	25%	17%	30%	0%	40%
Semi-annually	7%	6%	6%	0%		17%	25%	0%	17%	0%	0%	10%
Yearly	12%	10%	6%	17%		0%	0%	8%	0%	10%	17%	0%
Every few years	1%	0%										
Never	0%											
How often does the issuer test its Incident Response Plan (IRP)?												
Monthly	6%	7%	14%	17%		0%	25%	10%	20%	11%	0%	22%
Quarterly	15%	15%	21%	33%		25%	25%	20%	20%	22%	40%	11%
Semiannually	16%	16%										
Annually	51%	54%	57%	33%		75%	50%	60%	60%	56%	40%	67%
Every few years	7%	6%	7%	17%		0%	0%	10%	0%	11%	20%	0%
Never	2%	1%										
The issuer does not have an IRP	3%	1%										
How often does the issuer conduct tabletop simulations?												
Monthly	5%	6%	17%	17%		0%	25%	13%	20%	14%	0%	25%
Quarterly	11%	11%	17%	17%		33%	25%	13%	20%	14%	25%	13%
Semiannually	16%	15%	25%	17%		0%	25%	25%	40%	14%	25%	25%
Annually	48%	51%	33%	33%		67%	25%	38%	20%	43%	25%	38%
Every few years	11%	10%										
Never	10%	7%	8%	17%		0%	0%	13%	0%	14%	25%	0%
How does the issuer monitor for and/or detect cyber incidents?												
Managed Security Service Provider (MSSP)	17%	17%	21%	40%		0%	0%	27%	0%	33%	17%	25%
Security Operations Center (SOC)	31%	28%	43%	20%		67%	100%	27%	80%	22%	50%	38%
MSSP and SOC	42%	50%	36%	40%		33%	0%	45%	20%	44%	33%	38%
Other	9%	4%										
Issuer does not monitor for and/or detect cyber incidents	1%	0%										
Does the issuer participate in industry threat information sharing group?												
Yes	84%	76%	88%	67%		100%	100%	85%	100%	80%	71%	100%
No	16%	24%	13%	33%		0%	0%	15%	0%	20%	29%	0%
Does the issuer have a patch management policy in place?												
Yes	96%	98%	100%	100%		100%	100%	100%	100%	100%	100%	100%
No	4%	2%										
Does the issuer have a vulnerability management program?												
Yes	95%	96%	88%	83%		100%	100%	85%	100%	80%	86%	90%
No	5%	4%	12%	17%		0%	0%	15%	0%	20%	14%	10%

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
How often does the issuer conduct penetration tests?												
Monthly or more	22%	21%	27%	0%		50%	50%	18%	50%	11%	20%	30%
Quarterly	13%	14%	13%	0%		17%	50%	0%	33%	0%	0%	20%
Semi-annually	11%	13%	7%	20%		0%	0%	9%	0%	11%	20%	0%
Yearly	43%	46%	53%	80%		33%	0%	73%	17%	78%	60%	50%
Every few years	8%	5%										
Never	3%	0%										
How often does the issuer conduct red team/purple team engagements?												
Monthly or more	7%	7%										
Quarterly	7%	8%	21%	17%		20%	67%	9%	50%	10%	17%	25%
Semi-annually	7%	7%										
Yearly	27%	32%	36%	33%		40%	0%	45%	25%	40%	33%	38%
Every few years	18%	18%	14%	17%		20%	33%	9%	25%	10%	0%	25%
Never	34%	28%	29%	33%		20%	0%	36%	0%	40%	50%	13%
Does the issuer have a program for responding to external reports of security issues affecting the issuer's products or operations?												
Yes	55%	56%	79%	67%		80%	100%	70%	100%	67%	67%	88%
No	45%	44%	21%	33%		20%	0%	30%	0%	33%	33%	13%
Does the issuer provide compensation for external reports of security issues affecting the issuer's products or operations? (Only shown if answered "Yes" to question on line 150)												
Yes	26%	26%	33%	0%		33%	50%	20%	60%	0%	0%	50%
No	74%	74%	67%	100%		67%	50%	80%	40%	100%	100%	50%
Does the issuer have an insider threat program to detect and mitigate threats from employees and other individuals with access to the issuer's systems, data, or premises?												
Yes	77%	76%	80%	67%		80%	75%	82%	83%	78%	80%	80%
No	23%	24%	20%	33%		20%	25%	18%	17%	22%	20%	20%
How often does the issuer back up its data and/or systems to a resource that is disconnected from the issuer's network?												
Daily or more	78%	77%	77%	67%		80%	100%	70%	100%	70%	50%	100%
Weekly	11%	10%	23%	33%		20%	0%	30%	0%	30%	50%	0%
Monthly	5%	6%										
Quarterly	1%	2%										
Annually	1%	1%										
Every few years	0%											
Never	4%	5%										
Does the issuer scan back-up data for malware or other vulnerabilities?												
Yes	78%	77%	69%	67%		60%	75%	67%	75%	67%	67%	71%
No	22%	23%	31%	33%		40%	25%	33%	25%	33%	33%	29%
Does the issuer use an identity management service provider?												
Yes	80%	85%	64%	60%		80%	100%	50%	80%	56%	60%	67%
No	20%	15%	36%	40%		20%	0%	50%	20%	44%	40%	33%
Does the issuer have a policy that mandates that all applications go through an identity provider and enforce Multi-Factor Authentication?												
Yes	75%	83%	86%	80%		100%	100%	82%	100%	78%	80%	89%
No	25%	17%	14%	20%		0%	0%	18%	0%	22%	20%	11%
Does the issuer maintain a Priviledged Access Management program?												
Yes	85%	89%	92%	75%		100%	100%	89%	100%	88%	80%	100%
No	15%	11%	8%	25%		0%	0%	11%	0%	13%	20%	0%

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
Does the issuer have a policy to track, manage and risk assess End-of-Life (EOL) software?												
Yes	79%	82%	93%	100%		100%	100%	91%	75%	100%	100%	88%
No	21%	18%	7%	0%		0%	0%	9%	25%	0%	0%	13%
Does the issuer maintain a program that determines where open source software is used and embedded?												
Yes	41%	43%	64%	67%		60%	100%	55%	100%	50%	50%	75%
No	36%	33%	21%	17%		20%	0%	27%	0%	30%	33%	13%
N/a	24%	23%	14%	17%		20%	0%	18%	0%	20%	17%	13%
Does the issuer have a process to review and approve open source code within the software? (Only shown if answered "Yes" to question on line 182)												
Yes	81%	85%	100%	100%		100%	100%	100%	100%	100%	100%	100%
No	19%	15%										
Does the issuer monitor for and address cloud security misconfiguration?												
Yes	84%	88%	93%	100%		80%	100%	91%	100%	90%	83%	100%
No	16%	12%	7%	0%		20%	0%	9%	0%	10%	17%	0%
Does the issuer maintain a third party vendor cyber risk program?												
Yes	72%	75%	80%	67%		100%	100%	73%	100%	70%	67%	89%
No	28%	25%	20%	33%		0%	0%	27%	0%	30%	33%	11%
How frequently are vendors' cybersecurity risk practices reviewed?												
Monthly	8%	7%	31%	0%		25%	67%	20%	75%	11%	20%	38%
Quarterly	8%	10%										
Annually	49%	47%	31%	40%		50%	33%	30%	25%	33%	40%	25%
Every few years	22%	23%	23%	40%		25%	0%	30%	0%	33%	40%	13%
Never	14%	12%	15%	20%		0%	0%	20%	0%	22%	0%	25%
Does the issuer evaluate cyber risk from third-party software providers?												
Yes	89%	90%	93%	83%		100%	100%	91%	100%	90%	83%	100%
No	11%	10%	7%	17%		0%	0%	9%	0%	10%	17%	0%
How frequently does the issuer review third-party software providers' cyber risk programs?												
Quarterly	8%	9%	8%	0%		0%	33%	0%	33%	0%	0%	14%
Annually	49%	49%	58%	40%		75%	67%	56%	67%	56%	60%	57%
Bi-annually	3%	3%										
Every few years	26%	27%	33%	60%		25%	0%	44%	0%	44%	40%	29%
Never	14%	13%										
Does the issuer require that vendors (software providers and others) whose personnel or products have access to the issuer's IT systems carry cyber insurance?												
In a few cases (1% - 35%)	16%	20%	10%	20%		0%	0%	13%	0%	14%	25%	0%
In about half the cases (36% - 65%)	5%	6%	10%	20%		0%	0%	13%	0%	14%	25%	0%
In most cases (66% - 95%)	22%	23%	10%	20%		0%	0%	13%	0%	14%	0%	17%
In all cases (96% - 100%)	22%	17%	20%	20%		0%	50%	13%	33%	14%	25%	17%
Never	34%	33%	50%	20%		100%	50%	50%	67%	43%	25%	67%
Does the issuer have a Service Level Agreement with its critical vendors in place to be notified of an incident or newly identified vulnerability?												
Yes	84%	87%	93%	83%		100%	100%	91%	100%	90%	83%	100%
No	16%	13%	7%	17%		0%	0%	9%	0%	10%	17%	0%
Does the issuer require a cybersecurity assessment of a target company prior to completing an M&A transaction?												
Yes	43%	61%	77%	67%		80%	50%	82%	75%	78%	60%	88%
No	16%	18%	23%	33%		20%	50%	18%	25%	22%	40%	13%
N/a	41%	21%										

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
TRANSFER												
What percentage of the issuer's IT infrastructure is currently hosted on the public cloud?												
0%	8%	3%	0%	0%		0%	0%	0%	0%	0%	0%	0%
1%-10%	22%	17%	22%	40%		0%	0%	29%	0%	29%	20%	25%
10%-20%	13%	10%	11%	20%		0%	0%	14%	0%	14%	20%	0%
20%-30%	11%	11%	22%	20%		33%	0%	29%	0%	29%	40%	0%
30%-40%	7%	9%										
40%-50%	8%	10%	11%	20%		0%	0%	14%	0%	14%	0%	25%
50%-60%	7%	8%	11%	0%		33%	50%	0%	50%	0%	0%	25%
60%-70%	6%	6%	11%	0%		33%	0%	14%	0%	14%	20%	0%
70%-80%	7%	9%										
80%-90%	5%	7%										
90%-100%	7%	10%	11%	0%		0%	50%	0%	50%	0%	0%	25%
What percentage of the issuer's IT infrastructure does the issuer expect will be hosted on the public cloud 1 year from now?												
0%	6%	3%	0%	0%		0%	0%	0%	0%	0%	0%	0%
1%-10%	14%	10%										
10%-20%	13%	10%	33%	50%		0%	0%	38%	0%	38%	33%	33%
20%-30%	10%	9%	11%	17%		0%	0%	13%	0%	13%	17%	0%
30%-40%	9%	9%	11%	0%		33%	0%	13%	0%	13%	17%	0%
40%-50%	8%	9%	11%	17%		0%	0%	13%	0%	13%	17%	0%
50%-60%	7%	7%	11%	17%		0%	0%	13%	0%	13%	0%	33%
60%-70%	6%	6%	11%	0%		33%	100%	0%	100%	0%	0%	33%
70%-80%	9%	12%	11%	0%		33%	0%	13%	0%	13%	17%	0%
80%-90%	7%	10%										
90%-100%	10%	15%										
What percentage of the issuer's OT infrastructure is currently hosted on the public cloud?												
0%	60%	48%	0%	0%		0%	0%	0%	0%	0%	0%	0%
1%-10%	25%	29%										
10%-20%	4%	7%										
20%-30%	4%	7%										
30%-40%	0%	1%										
40%-50%	0%	1%										
50%-60%	3%	4%										
60%-70%	0%											
70%-80%	1%	1%										
80%-90%	1%	1%										
90%-100%	1%	2%										

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
What percentage of the issuer's OT infrastructure does the issuer expect will be hosted on the public cloud 1 year from now?												
0%	54%	41%	0%	0%		0%	0%	0%	0%	0%	0%	0%
1%-10%	23%	27%										
10%-20%	8%	9%										
20%-30%	5%	9%										
30%-40%	2%	3%										
40%-50%	1%	3%										
50%-60%	1%	2%										
60%-70%	0%											
70%-80%	1%	1%										
80%-90%	2%	1%										
90%-100%	2%	3%										
Does the issuer carry standalone cyber insurance?												
Yes	80%	83%	92%	100%		100%	100%	90%	75%	100%	100%	86%
No	20%	17%	8%	0%		0%	0%	10%	25%	0%	0%	14%
Does the issuer's standalone cyber insurance policy include system failure coverage? (Only shown if answered "Yes" to question on line 273)												
Yes	82%	85%	73%	60%		100%	100%	67%	100%	67%	67%	80%
No	18%	15%	27%	40%		0%	0%	33%	0%	33%	33%	20%
Does the issuer expect to buy more, the same, or less standalone cyber insurance limit in 2025? (Only shown if answered "Yes" to question on line 273)												
More	15%	14%										
The same	85%	85%	100%	100%		100%	100%	100%	100%	100%	100%	100%
Less	1%	1%										
What is the expected percentage increase in standalone cyber insurance limit?												
1%-10%	31%	30%										
10%-25%	35%	32%										
25%-50%	19%	25%										
More than 50%	15%	14%										
Does the issuer expect the price of standalone cyber insurance to increase, decrease, or stay the same when they renew their policy? (Only shown if answered "Yes" to question on line 273)												
Increase	42%	30%	42%	60%		20%	33%	44%	33%	44%	50%	33%
Decrease	13%	17%	8%	20%		0%	0%	11%	0%	11%	17%	0%
Stay the same	45%	53%	50%	20%		80%	67%	44%	67%	44%	33%	67%
Has the issuer issued a public notice of a cyber incident in the last 12 months?												
Yes	8%	7%	7%	17%		0%	0%	8%	0%	10%	0%	13%
No	92%	93%	93%	83%		100%	100%	92%	100%	90%	100%	88%

				Region (Autos)			Sub-sectors (Autos)		Size (Autos)		Rating tranche (Autos)	
	Global	CFG	Autos	Americas	Asia Pacific	Europe, Middle East & Africa	Automobile Manufacturers	Automotive Suppliers	Large	Small	High Yield	Investment Grade
ARTIFICIAL INTELLIGENCE												
Does the issuer have a policy governing the use of AI tools?												
Yes	68%	78%	87%	83%		100%	67%	92%	80%	90%	83%	89%
No	26%	19%	13%	17%		0%	33%	8%	20%	10%	17%	11%
N/a	5%	3%										
Does the issuer have a policy restricting the use of internal and/or proprietary data with public AI tools?												
Yes	73%	82%	88%	83%		83%	75%	92%	83%	90%	83%	90%
No	22%	15%	6%	17%		0%	0%	8%	0%	10%	17%	0%
N/a	6%	4%	6%	0%		17%	25%	0%	17%	0%	0%	10%
Has the issuer established restricted, internal-use generative AI tools?												
Yes	64%	74%	92%	83%		100%	100%	91%	100%	90%	83%	100%
No	36%	26%	8%	17%		0%	0%	9%	0%	10%	17%	0%
Is the issuer following OWASP Top 10 for its use of generative AI?												
Yes	29%	32%	36%	0%		50%	50%	33%	67%	25%	20%	50%
No	36%	36%	55%	100%		25%	0%	67%	0%	75%	80%	33%
N/a	35%	32%	9%	0%		25%	50%	0%	33%	0%	0%	17%

Endnotes

1 System failure coverage provides indemnification for net income loss and extra expenses associated with a degradation or failure in technology not caused by a cyberattack; this type of coverage is crucial for protecting against non-malicious losses that can disrupt business operations

within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the issuer/deal page on https://ratings.moodys.com for the most updated credit rating action information and rating history.

REPORT NUMBER 1469550

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454