ESET SMB Cyber Readiness Index 2026

Global edition

Cybersecurity
Progress. Protected.

Message From The VP

Michal Jankech

Vice President of Enterprise, SMB & MSP

Your company may be a small and medium-sized business (SMB), but its threat surfaces reflect a much larger reality.

As it stands, meeting cybersecurity challenges in 2026 means understanding the intersection of your business needs, human behavior, the democratization of powerful technologies like AI, regulatory priorities and the rather volatile threat landscape—that's a lot! Therefore, to face all of these, there is but one choice—to become more resilient—starting with charting one's own state of readiness.

On behalf of the thousands of SMBs ESET supports, and their peers, which make up 90% of global economic activity, we've taken this snapshot of cyber readiness to highlight the progress made toward meeting both persistent challenges, as well as lessons learned on emerging issues. These are mapped in the index to document recent SMB security decisions as they chart a course toward improved resilience.

Table Of Contents

The 2026 ESET Cyber Readiness Report is structured in five sections, drawing together comparative data on global and regional results. Where country-level data stands out, it has been included to offer additional insight on the evolving concerns and choices of SMBs in the security space.

1

Headline Stats

Global Headline Stats 1/2

61% of organizations fear an attack in the next year

Most Concerning Threats

AI-powered malware (31%), Ransomware and malware (29%), Phishing / Spear phishing (26%).

Business Impact Concerns

Data loss (50%), operational disruption (40%), and financial impact (37%).

Resilience

75% are confident in their resilience (26% very, 49% slightly).

Incidents

45% of firms experienced an incident last year.

Reporting

36% reported incidents to cyber insurers, 30% to regulators, 29% to business partners, 28% to customers; 5% did not report.

Investigation & Recovery

41% in less than 2 weeks; 34% took two to six weeks.

Incident Causes & Challenges

Phishing as leading cause (26%), unpatched vulnerabilities (23%), lack of security monitoring (22%), weak passwords (20%). Main challenge: keeping up with new threats (34%) and latest tech like AI (32%).

Insurance

71% carry cyber insurance (37% with specific security control requirements). Specific requirements strictest at firms with multiple incidents (55%).

Global Headline Stats 2/2

Training & Awareness

- 87% consider training critical or very important.
- 42% use quality programs including phishing simulations; 28% use comprehensive training (usage of this type grows with company size).
- 53% train several times a year; 14% monthly. Adoption is highest at SMBs experiencing multiple incidents (81%), followed by those with 500-1000 endpoints (75%).

Investment & Resources

- 80% view their cybersecurity budget as sufficient or more than sufficient. 40% expect a budget increase next year.
- Top planned investments include employee training & awareness (41%), cloud security (33%) and backup & recovery (26%).
- Main obstacles are budget limits (24%), complexity / integration challenges (21%) and talent / skills shortages (20%).

AI & Future

- Perception: 75% agree cyber warfare is a real business threat. Only 31% feel safe relying solely on insurance.
- AI Integration: 73% are integrating AI, though 70% acknowledge it introduces new risks. 60% have an AI policy, which correlates with higher cybersecurity incident rates.
- Strategy: SMBs want to use AI primarily to anticipate threats and for faster attack mitigation.

EMEA Headline Stats 1/2

64% **of organizations fear an attack in the next year**

Most Concerning Threats

AI-powered malware (31%), identity/credential theft (27%), and ransomware / malware (27%), phishing / spear phishing (27%).

Business Impact Concerns

Data loss (51%), operational disruption (41%), and financial impact (38%).

Resilience

76% are confident in their resilience (26% very, 50% slightly).

Incidents

44% of firms experienced an incident last year.

Reporting

36% reported incidents to cyber insurers, 29% to regulators, 27% to customers, 27% to law enforcement; 7% did not report.

Investigation & Recovery

33% took two to six weeks; 43% took under two weeks.

Incident Causes & Challenges

Phishing was the leading incident (27%), unpatched vulnerabilities (23%), weak passwords & lack of security monitoring (20% each). Main challenge: keeping up with new tech like AI and new threats (both 32%).

Insurance

69% carry cyber insurance (34% with specific security control requirements). Specific requirements are strictest for firms with multiple past incidents (52%).

EMEA Headline Stats 2/2

Training & Awareness

- 87% consider training critical or very important.
- 43% use quality programs including phishing simulations; 26% use comprehensive training (usage of this type grows with company size).
- 51% train several times a year; 12% monthly. Adoption is highest at SMBs with 500-1000 endpoints (81%), followed by those experiencing multiple incidents (79%).

Investment & Resources

- 83% view their cybersecurity budget as sufficient or more than sufficient. 39% expect a budget increase next year.
- Top planned investments include employee training & awareness (40%), cloud security (33%) and Backup & recovery (25%).
- Main obstacles are budget limits (26%), complexity / integration challenges (20%) and talent / skills shortages (18%).

AI & Future

- Perception: 74% agree cyber warfare is a real business threat. Only 31% feel safe relying solely on insurance.
- AI Integration: 71% are integrating AI, though 70% acknowledge it introduces new risks. 57% have an AI policy, which correlates with higher cybersecurity incident rates.
- Strategy: SMBs want to use AI primarily to anticipate threats and for faster attack mitigation.

NORAM Headline Stats 1/2

62% of organizations fear an attack in the next year

Most Concerning Threats

AI-powered malware (33%), identity/credential theft (26%), and ransomware / malware (25%).

Business Impact Concerns

Data loss (44%), financial impact (41%) and operational disruption (41%).

Resilience

86% are confident in their resilience (41% very, 45% slightly).

Incidents

51% of firms experienced an incident last year.

Reporting

40% reported incidents to cyber insurers, 36% to business partners, 32% to customers, 31% to regulators; only 2% did not report.

Investigation & Recovery

40% took two to six weeks; 35% took under two weeks.

Incident Causes & Challenges

Phishing and lack of security monitoring (25% each) are leading causes. Main challenges: keeping up with new threats (41%), new tech like AI (37%).

Insurance

84% carry cyber insurance (51% with specific security control requirements). Specific requirements are for SMBs with multiple past incidents (71%).

NORAM Headline Stats 2/2

Training & Awareness

- 93% consider training critical or very important.
- 44% use quality programs including phishing simulations; 36% use comprehensive training (usage of this type grows with company size).
- 57% train several times a year; 23% monthly. Adoption is highest among firms that had multiple incidents (84%).

Investment & Resources

- 93% view their cybersecurity budget as sufficient or more than sufficient. 47% expect a budget increase next year.
- Top planned investments include employee training & awareness (42%), cloud security and backup & recovery (both 31%).
- Main obstacles are complexity / integration challenges (26%), budget limits (22%) and talent / skills shortages (18%).

AI & Future

- Perception: 82% agree cyber warfare is a real business threat. Only 36% feel safe relying solely on insurance.
- AI Integration: 77% are integrating AI, though 76% acknowledge it introduces new risks. 68% have an AI policy, which correlates with higher cybersecurity incident rates.
- Strategy: Primarily, SMBs want to use AI to anticipate threats and for faster attack mitigation.

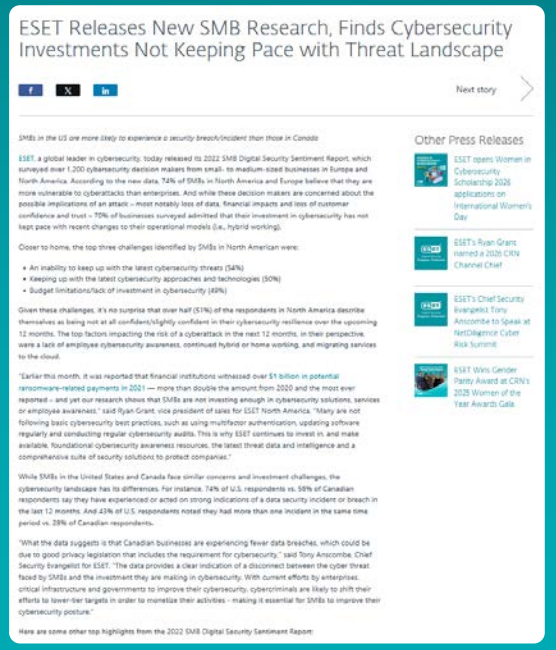
2

Road To Resilience In The Current Threat Landscape

Road To Resilience

ESET's 2022 SMB Sentiment Survey was published Nov. 11 – just two weeks before ChatGPT emerged and before Managed Detection and Response became a widely used service by SMBs.

Three years on, we've returned to understand how SMBs are navigating their security choices.


ESET Releases New SMB Research, Finds Cybersecurity Investments Not Keeping Pace with Threat Landscape

Next story

Other Press Releases

ESET opens Women in Cybersecurity Scholarship 2026 applications on International Women's Day

ESET's Ryan Grant named a 2026 CRN Channel Chief

ESET's Chief Security Evangelist Tony Anscombe to Speak at NetDiligence Cyber Risk Summit

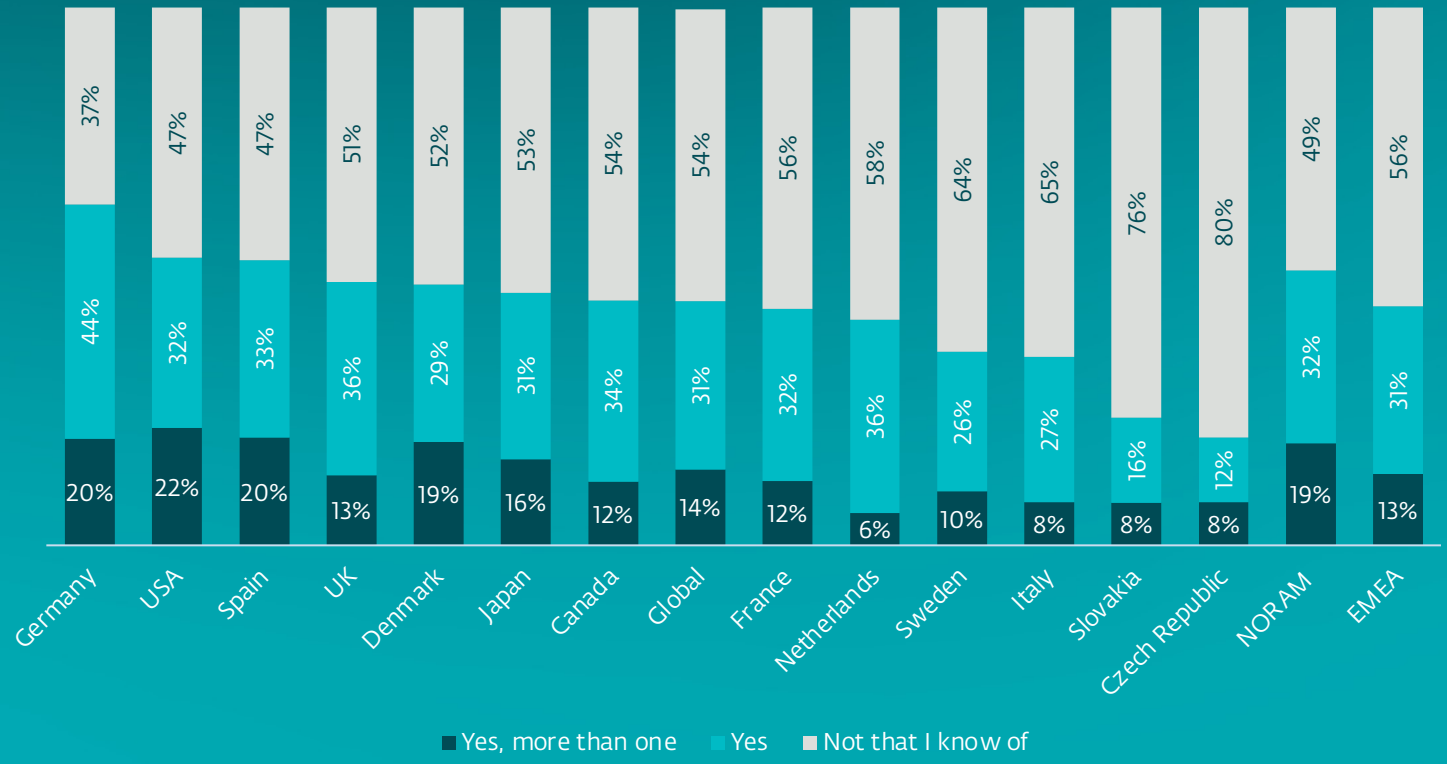
ESET Wins Gender Parity Award at CRN's 2025 Women of the Year Awards Gala

- Democratized access to technologies like AI, maturation of collaboration platforms and the highly evolved theater of cyber warfare have combined to make 2026 a very different security moment.
- SMBs have had to change their security posture, and it's put pressure on budgets and technology choices needed to become – and stay – resilient.
- In this survey we set out to discover how all this change has affected the leading security concerns for SMBs in 2026.

Old Wisdoms Hold True, Incident Rates Confirm That Smaller Businesses Aren't Immune To Attacks

- Nearly every second SMB surveyed (45%) communicated that they experienced an incident in the last 12 months.
- Germany leads with the highest rate of recorded incidents (one or more), followed by the USA and Spain.
- UK, Denmark, Japan and Canada follow – all are above the global results.
- France, the Netherlands, Sweden and Italy fall below the global results.

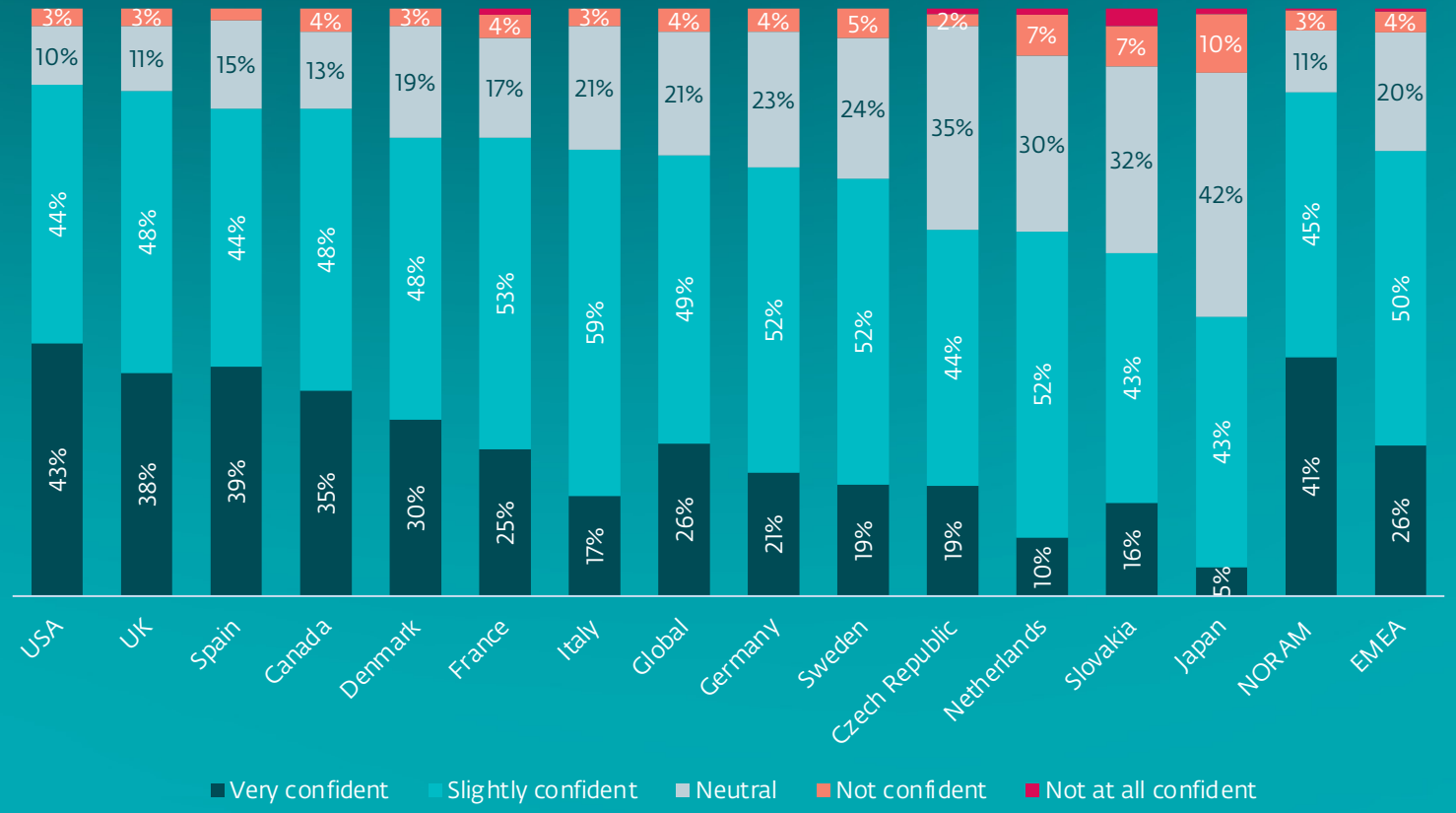
Cybersecurity incident experience in the last 12 months



Globally, A Majority Of SMBs Are Confident About Their Resilience

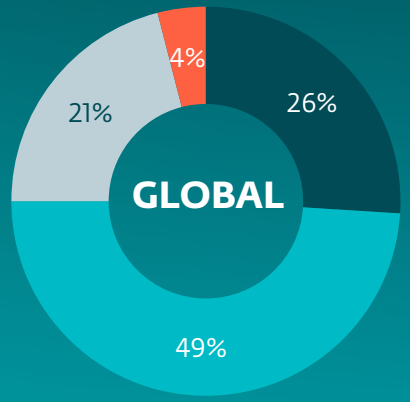
- The US and UK respondents lead with the highest confidence.
- European respondents led by Spain, Denmark, France and Italy also score above the global benchmark, with Germany and Sweden following, but just below.
- Japan is an outlier with a low number of “very confident” responses, and, conversely, a very high rate of “neutral” responses.
- Overall confidence (87%) rose significantly in comparison to our 2022 survey (48%).

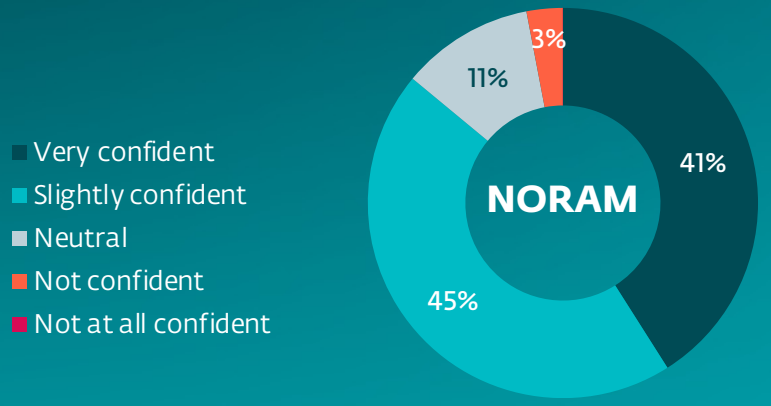
Confidence in the business: cyberattack resilience



North American businesses are more confident than the rest of the globe. Those that have already been exposed to more than one incident in North America (91%) and those exposed to more than one incident globally also demonstrate higher confidence (81%).

Confidence in the business: cyberattack resilience





Very confident
Slightly confident
Neutral
Not confident
Not at all confident

(values in %)

25-99 endpoints (n=1,796)	23	49	22	5
100-499 endpoints (n=1,581)	25	48	22	4
500-1,000 endpoints (n=1,023)	30	47	19	3
Experienced more than one incident (n=637)	36	45	14	4
Experienced one incident (n=1,378)	23	53	19	4
Did not experience incident (n=2,385)	24	47	24	4

(values in %)

25-99 endpoints (n=257)	38	45	13	5
100-499 endpoints (n=260)	42	48	8	2
500-1,000 endpoints (n=183)	44	42	10	4
Experienced more than one incident (n=133)	50	41	5	3
Experienced one incident (n=225)	38	48	12	3
Did not experience incident (n=342)	39	45	12	4

Globally, Concerns Over The Threat Landscape Are Largely Similar

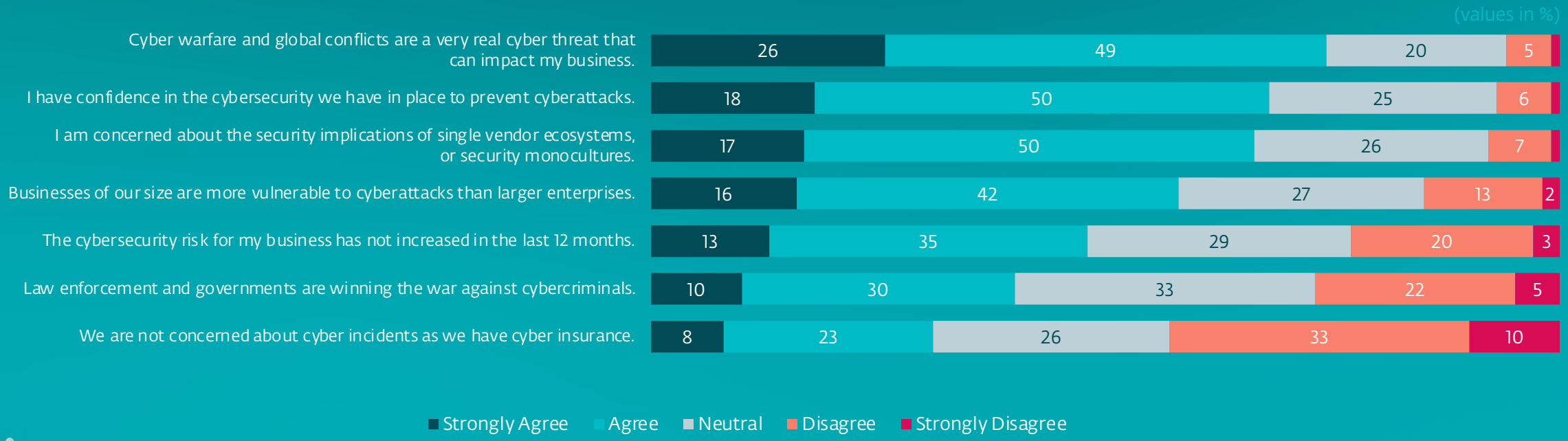
Cyber warfare

SMBs might have confidence in their security, but 75% of SMBs agree that global conflicts and cyberwarfare feel very close.

Vendor Consolidation

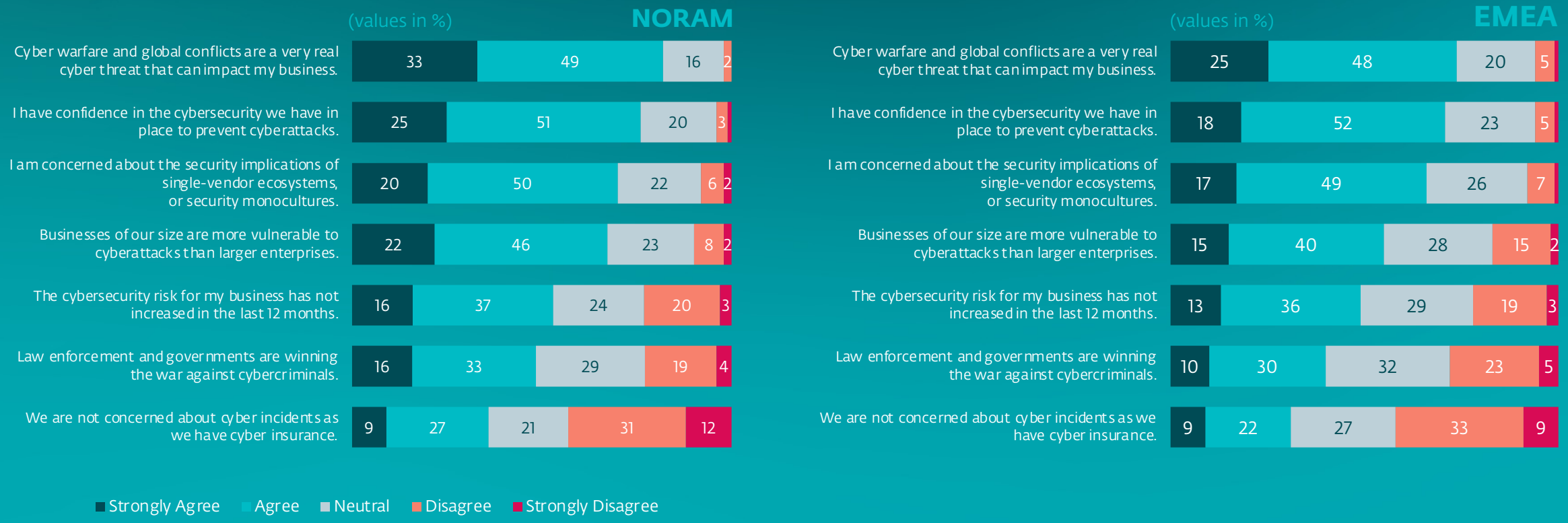
Another worry is cyber vendor consolidation: 67% of SMBs worry about single vendor ecosystems and monocultures.

To what extent do you agree with the following statements?



North American SMBs demonstrate higher threat awareness – more of them understand that cyberwarfare can impact their business and being small isn't a protection against cyberattacks. At the same time, they also have higher confidence in their ability to prevent attacks.

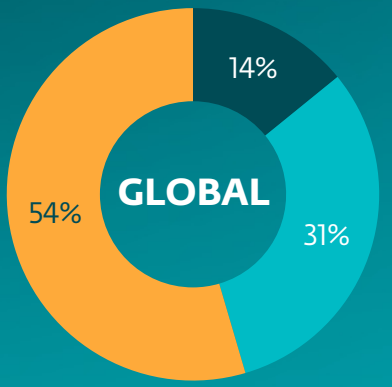
To what extent do you agree with the following statements?



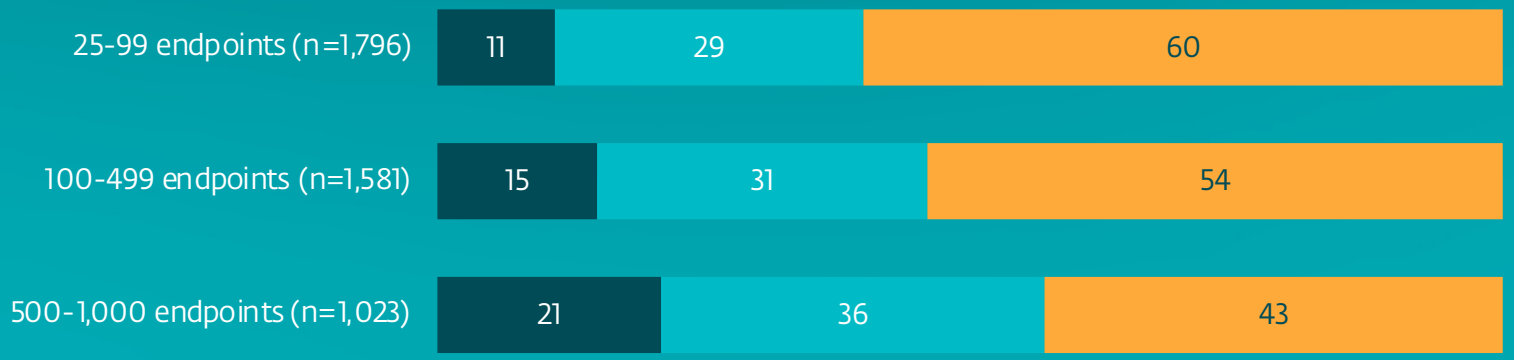
Nearly Half Of SMBs Globally Have Suffered At Least One Incident In The Last Year

- Globally, the majority of SMBs that have more than 500 endpoints have experienced one or more incidents.
- The smallest SMBs surveyed, those with 25-99 endpoints, responded that they experienced 30% fewer incidents than those with 500 – 1,000 endpoints.

Cybersecurity incident experience in last 12 months

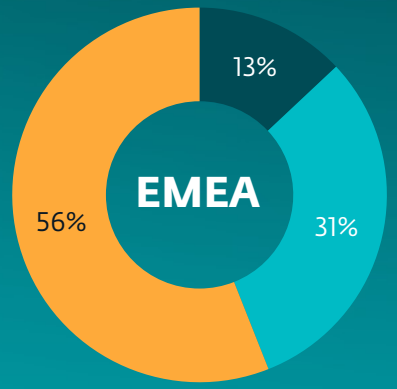


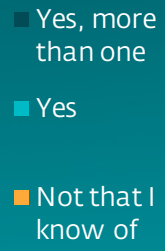
(values in %)

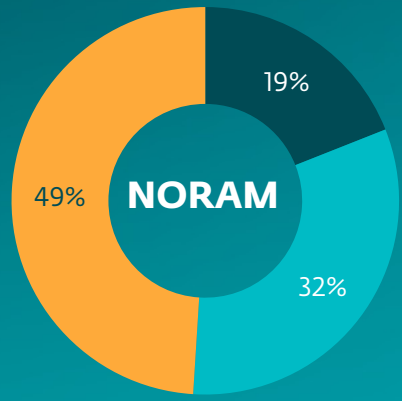


SMBs in North America experienced a higher number of incidents than countries globally, particularly larger businesses.

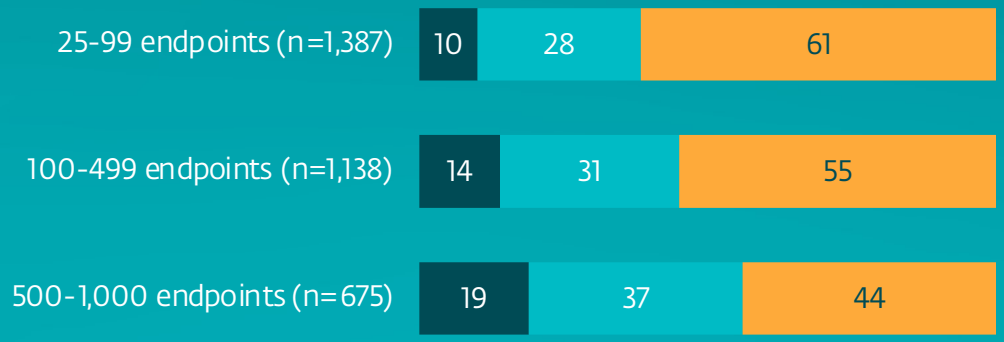
Cybersecurity incident experience in last 12 months



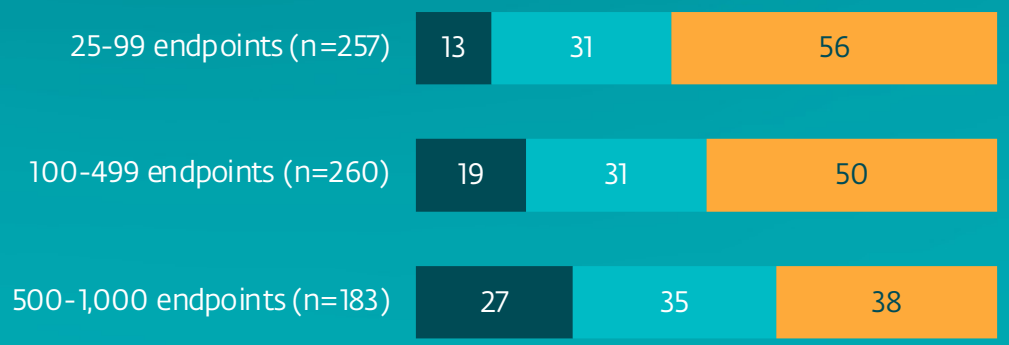




(values in %)



(values in %)

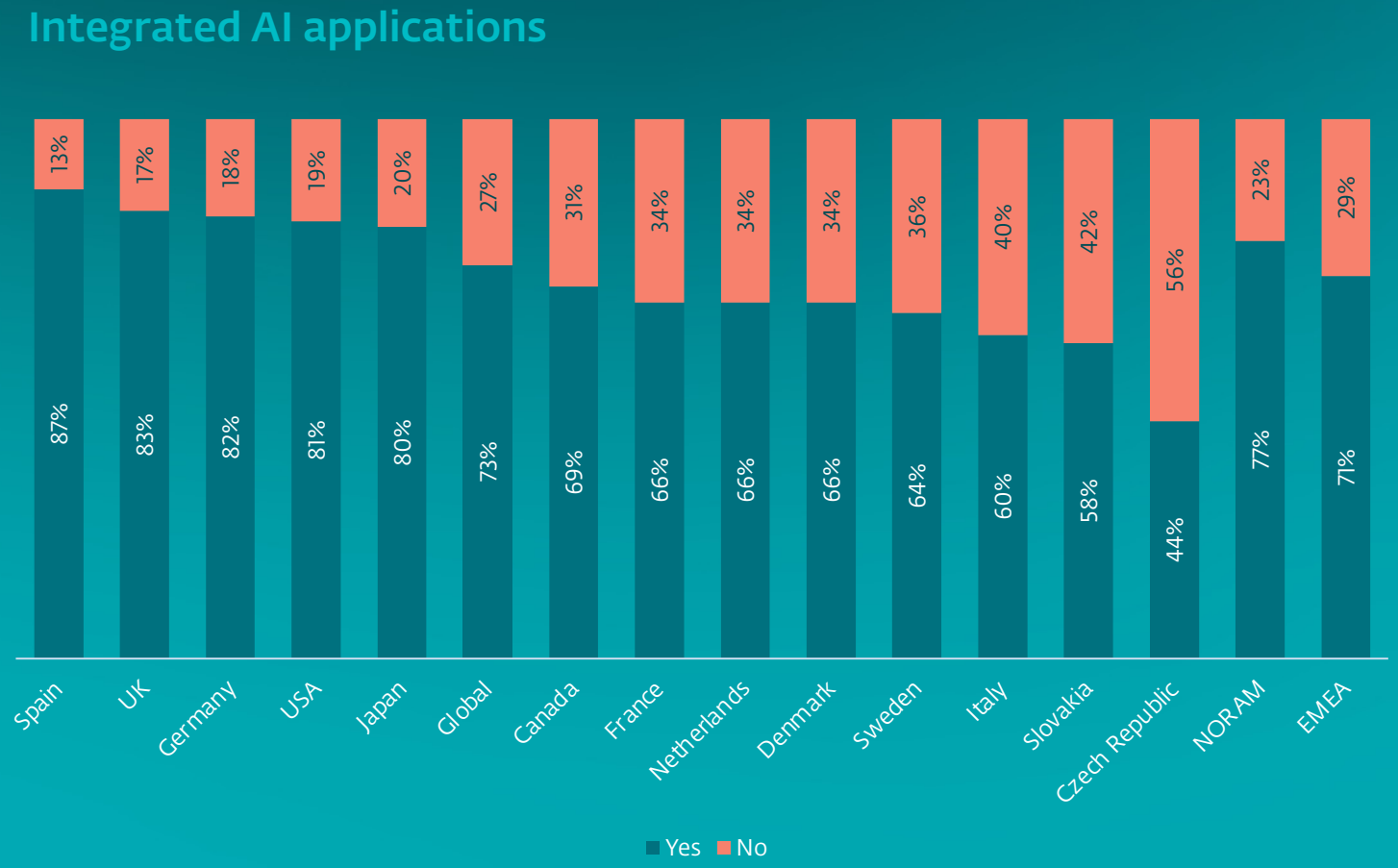


3

Does The Road To Resilience Pass Through AI?

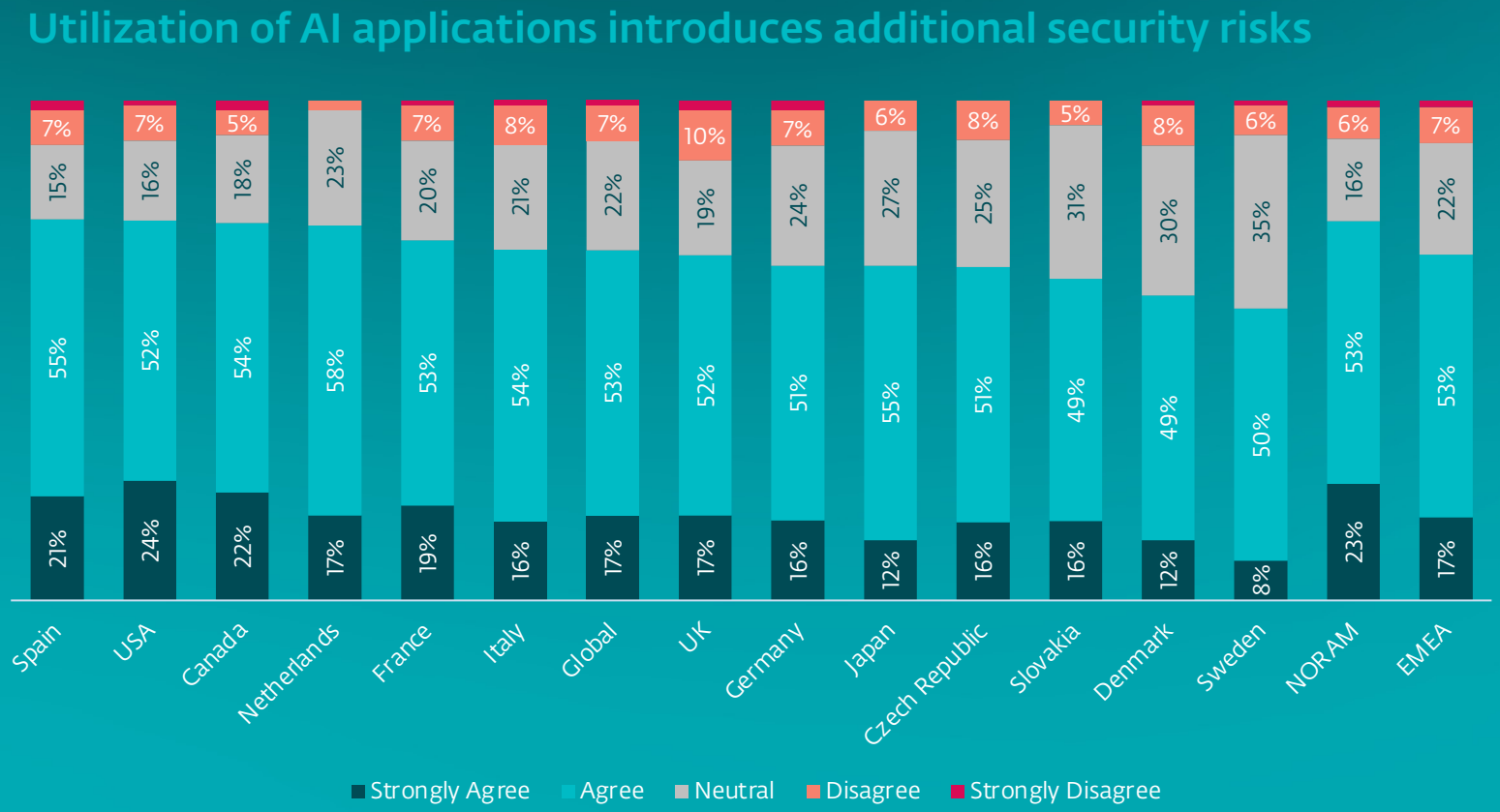
Global Appetite For AI Integration Varies

- While North America demonstrated a slight edge (77%) in AI integration compared to the global results (73%), integration of AI among European businesses reached 71%.
- Appetite for AI integrations at the country level was diverse in Europe, with SMBs in Spain leading globally at 87%, followed by the UK at 83%.



Security Concerns Are Not At The Root Of AI Adoption Enthusiasm – Or Distrust

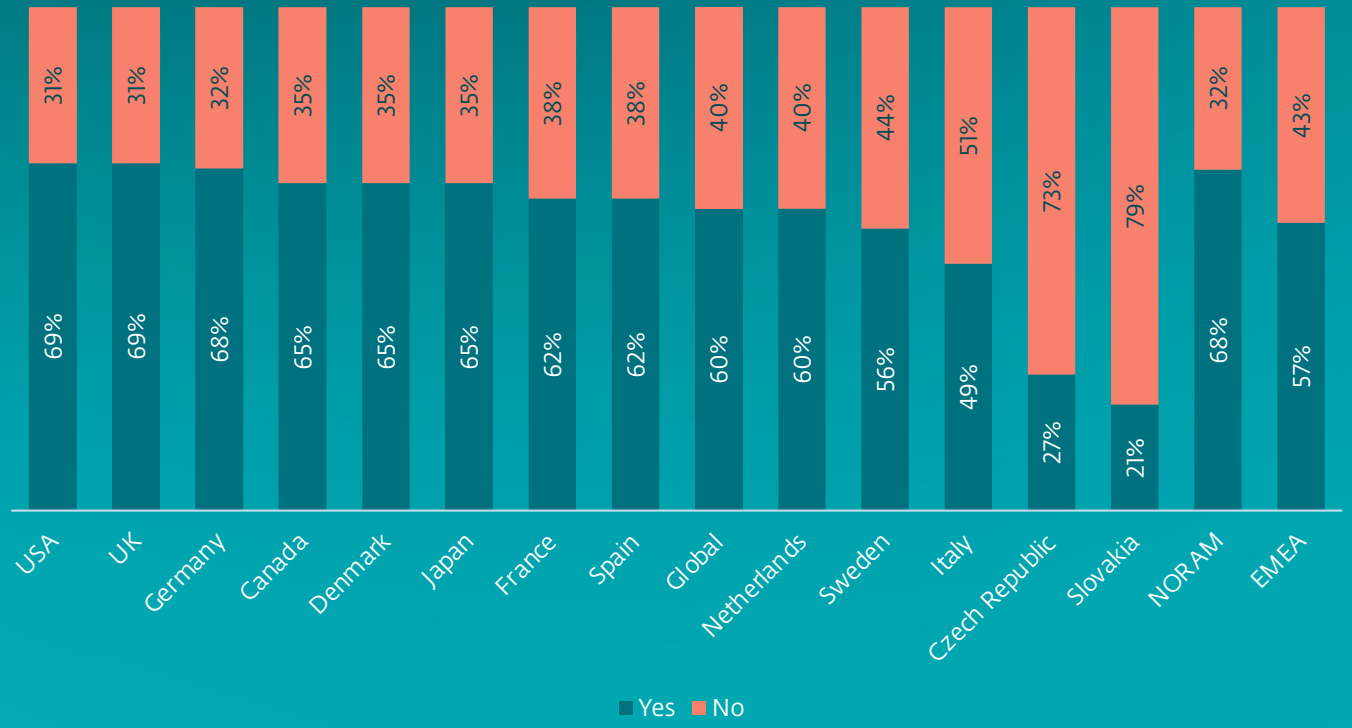
- Globally, Spain leads in awareness of security risks vectoring from AI.
- Their SMB peers in the USA, Canada, Netherlands, France and Italy follow closely with solid utilization and awareness.



Enthusiastic AI Adoption Comes With Proactive Shadow AI Policies – With Two Central European Exceptions

- SMBs in the US, UK and Germany reported the most limited shadow AI.
- Overall countries with higher AI integration and utilization rates also have better implementation of AI policies. Four of the thirteen countries surveyed fall below the global results regarding implementation of restrictive AI policies.
- In Slovakia, awareness of risks from AI is high, while policies limiting shadow AI are very low. Conversely, while Czech respondents' slower rollout was visible, they were more risk aware and more likely to restrict AI applications than Slovak respondents.

AI policy to restrict use of AI applications outside approved processes or platforms (shadow AI)



Perception VS Reality: Are SMBs Worried About The Right Threats?

01

SMBs say AI-powered malware is their top concern for the year ahead, a signal of how dominant AI has become in headlines and boardroom conversations.

02

However, the actual causes of incidents paint a very different picture – pointing to phishing, a lack of security monitoring, unpatched security vulnerabilities and weak passwords as the drivers for incidents.

03

Meanwhile, one of the most consequential risks - supply chain compromise - barely registers among SMBs' top concerns, despite the potential for widespread downstream impact.

Concerns Over AI-Powered Malware Are High… But Misplaced

0 The ESET MDR dataset contains zero incidents in which generative AI played a significant role. While many threats benefit from AI support, operational AI, leveraged in real time for automated tasks, remains rare.

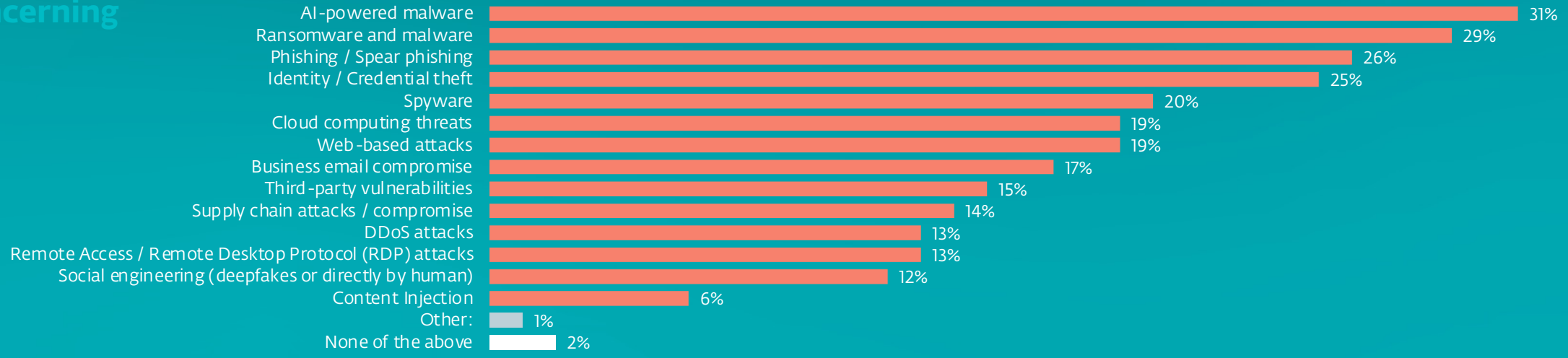
There's plenty of news about AI-powered malware. It's not surprising that many businesses worry about it.

AI-powered malware is rare in the wild. It is defined as malware that uses AI in an automated and real-time (on-the-fly) manner.

Right now, AI-powered malware is a hot topic for malware researchers – not SMBs' IT teams.

More on these ESET Discoveries:
- →PromptLock – 1st AI-powered ransomware, experimental
- →PromptSpy – 1st Android malware of this kind, uses AI to achieve persistence

Most concerning threats

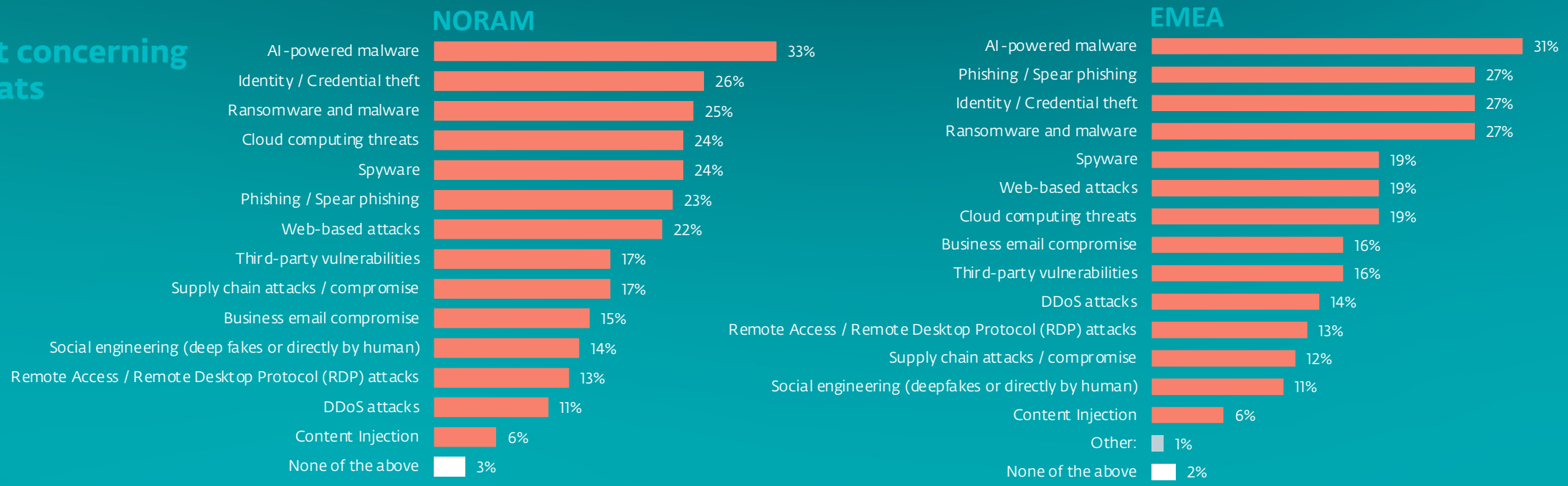


While SMBs in both EMEA and North American regions are almost equally concerned about AI-powered malware, they differ slightly in their opinion about other threats.

North American businesses are more concerned with supply chain attacks and worry less about phishing.

Further data in this report show that North American businesses are more confident when it comes to identifying phishing, and in their employees' awareness, as they utilize higher tiers of cybersecurity awareness training.

Most concerning threats



AI-Powered & Driven

- The biggest current threat involving AI is its use by attackers to automate parts of existing attacks – in much the same way that office workers use it to automate dull, simple or repetitive tasks.
- For attackers, AI is currently a tool that makes it easier and faster to create and operate malicious campaigns.
- The real-world outcome? Higher volumes of more convincing phishing messages and a rapid increase in new malware variants circulating in the wild.

We can observe that any direct use of AI to generate malware and scripts remains limited and specific. In reality the transformation in the threat landscape is taking place around social engineering and the overall acceleration of attacks, including supply-chain threats. However, with improving quality in coding agents, just as it is with standard software development, we anticipate a similar boost in malware development.

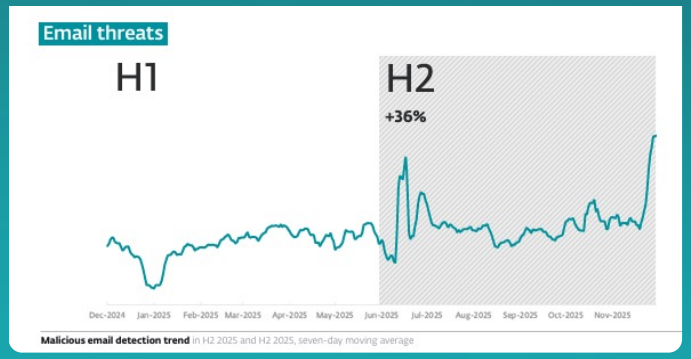
It is clear that the most significant challenge remains the continuous surge in high-quality messaging that includes AI-generated attack vectors, such as convincing deepfakes, emails and ads together with automation of attacks, environmental research, identification of vulnerabilities and automation of their exploitation. All of these improvements enable even low-skilled attackers to orchestrate sophisticated scams at scale and low cost as they receive capabilities that were previously available only to the APT world.

Attackers increasingly rely on automation and creating the appearance of trustworthiness rather than achieving genuine AI functionality, leveraging AI to mimic Professional-grade presentations and interactions – making social engineering one of the primary battlegrounds in cyber defense.

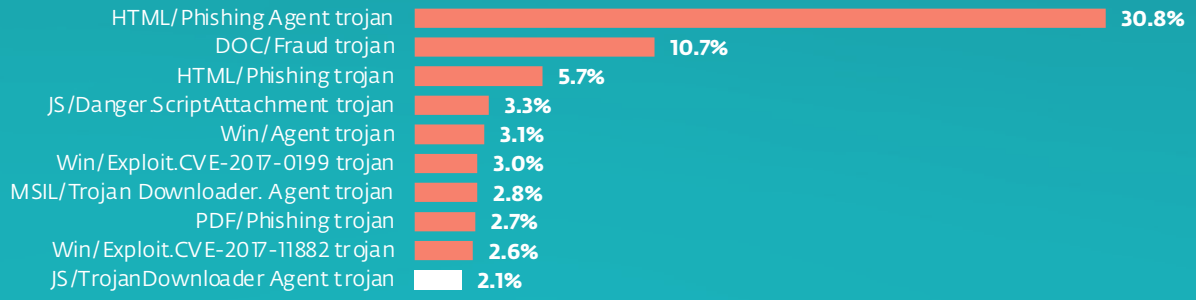
Juraj Jánošík
ESET VP of Artificial Intelligence

Globally, Phishing Is Still Number One

Phishing in ESET telemetry

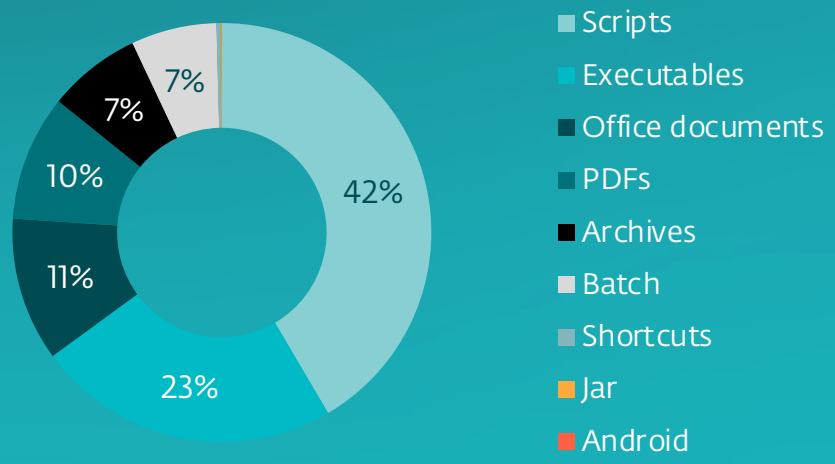


ESET telemetry shows that phishing is the top threat detected and the number of detections is rising, according to the ESET Threat Report H2 2025.



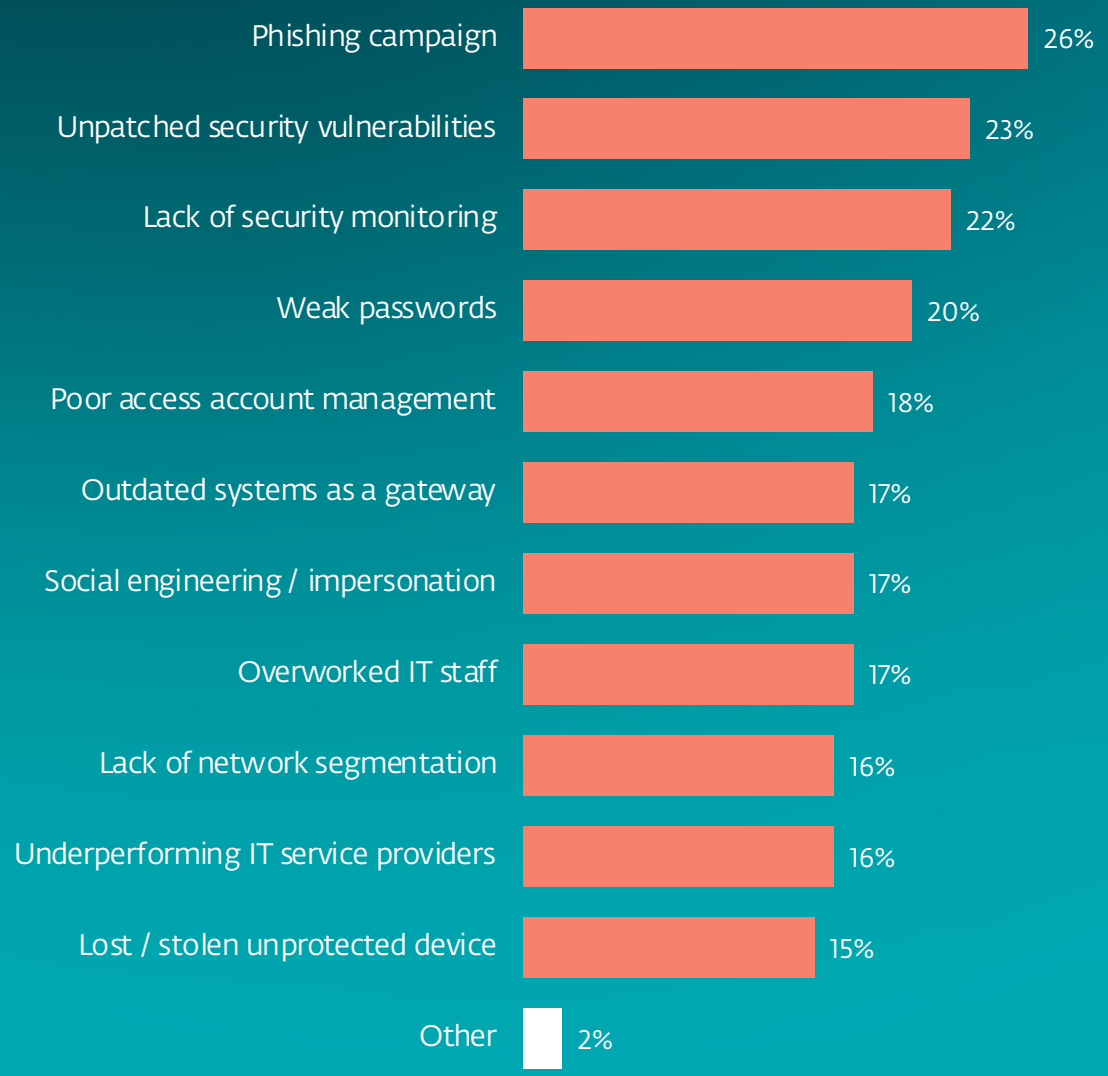
Top 10 threats detected in emails in H2 2025

Naturally, phishing is also reflected in the number of email threats.

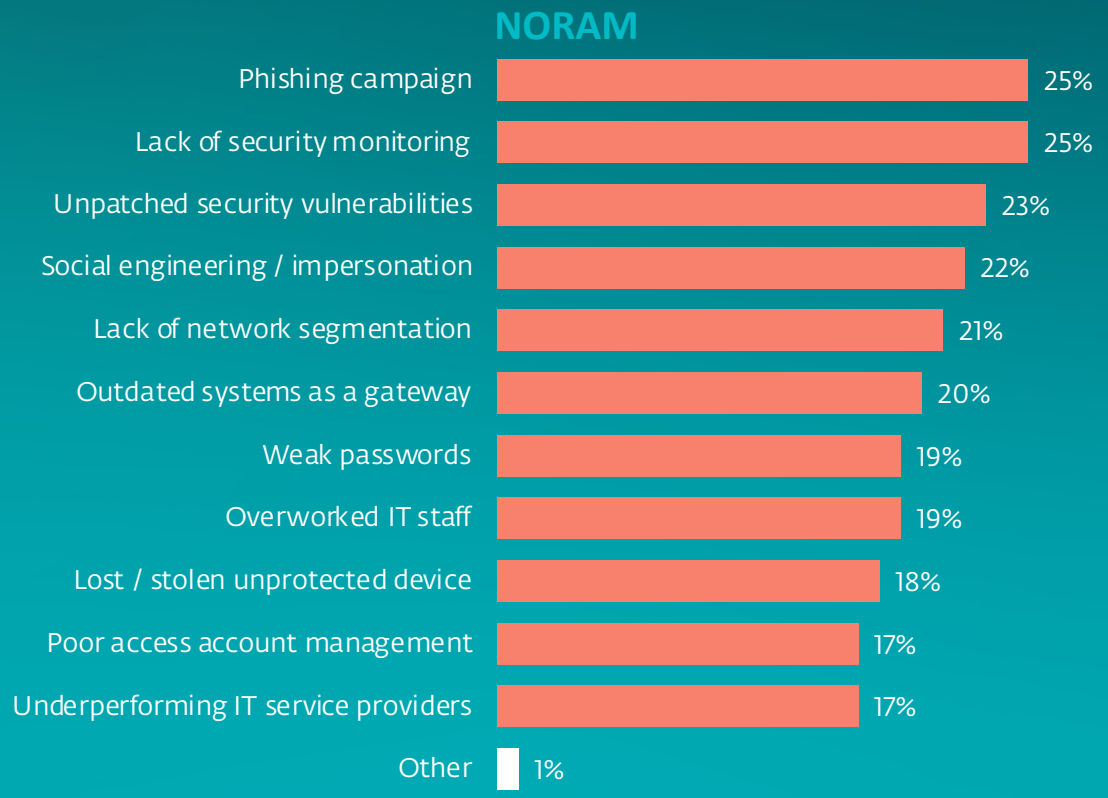


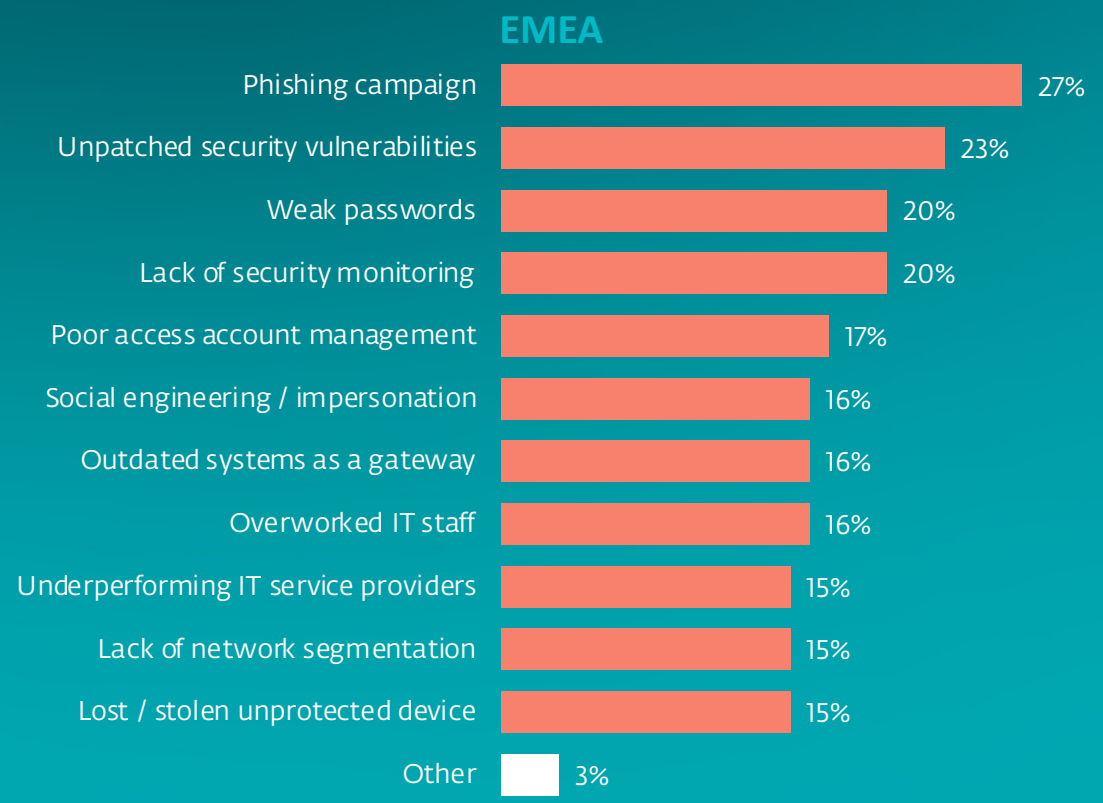
It’s Not AI – It’s The Same Old Cyber Threats, Automated

- Respondents are worried about AI malware.
- But instead, they need to prepare for increased volumes of the same old threats, now automated and accelerated by AI tools.



While the most common reasons for cybersecurity incidents are same for all surveyed regions, businesses in NORAM are clearly more often targeted by social engineering/impersonation. They also more often face problems within their systems, like lack of security monitoring and lack of network segmentation.

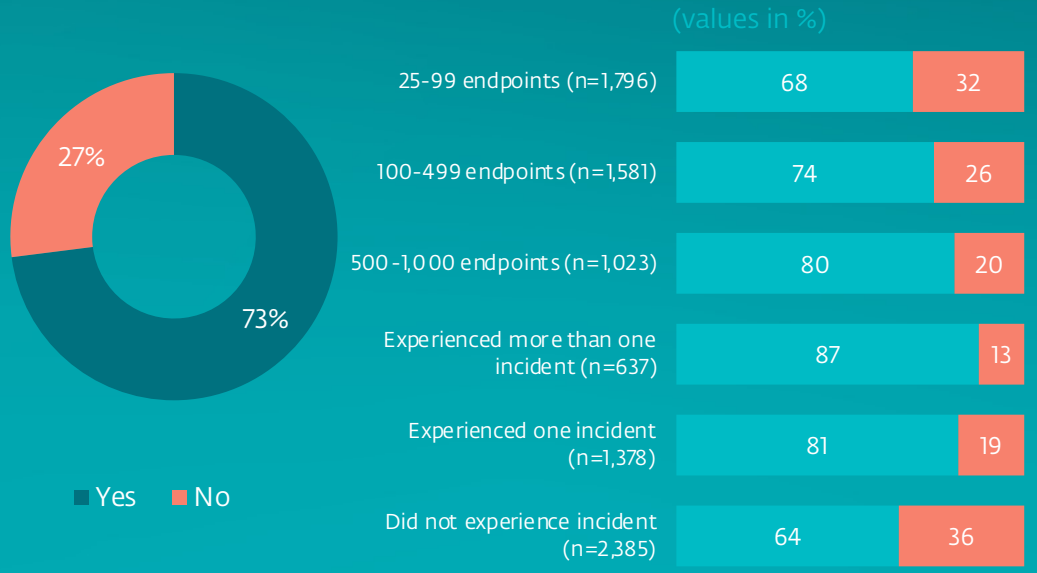




In-house AI, Whether You Want It Or Not: The Insider Threat

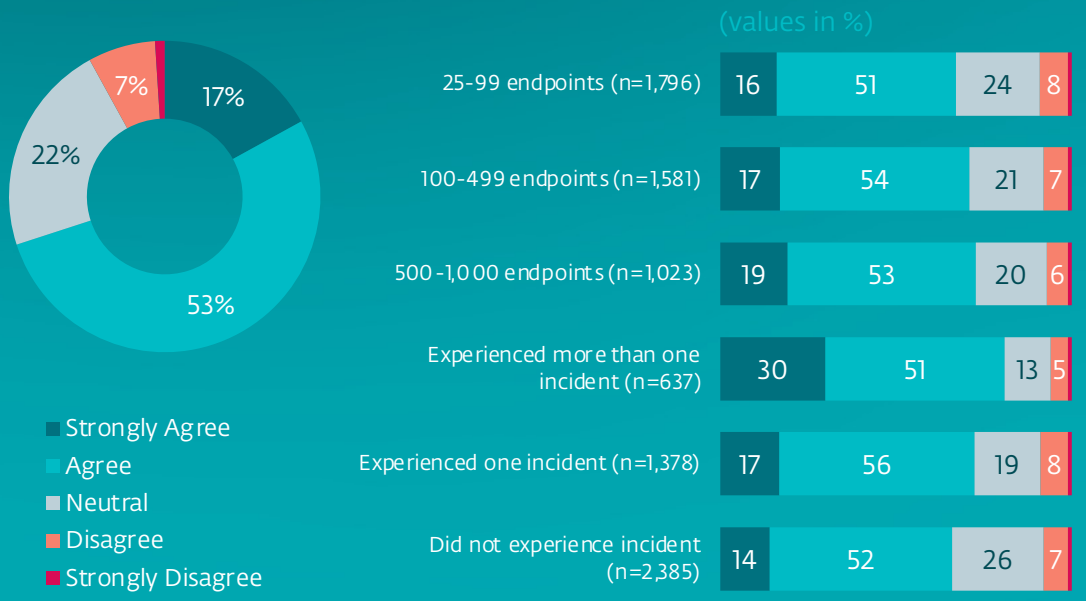
- In just three short years, AI has revolutionized how employees accomplish everyday work tasks. Many businesses have integrated AI tools to increase effectiveness.
- But just like any other fresh tech, AI tools attract cybercriminals. Surveyed SMBs seem to be aware of risks related to AI integration.
- Notably, businesses that experienced more incidents integrate AI more often and have higher awareness of related risks.

Integrated AI applications



Agreement with the statement:

"Utilization of AI applications introduces additional security risks"



Emerging AI Tools & Agents

- AI tools and agents can be effective “colleagues,” but attackers can trick them and abuse their privileges.
- For example, ESET has documented AI-related attacks abusing publicly available agentic skills,* turning AI agents into insider threats within a compromised system.
- Learn more - ESET Blog Post: The security crisis brewing in AI agent platforms

*An AI skill is a set of instructions, scripts and/or reference materials that can substitute a complicated series of prompts - effectively simplifying work with AI agents. Thousands of such skills are being added daily.

1.

Scanning of 60,000 publicly available skills found that thousands of them are at least suspicious and hundreds are straightforwardly malicious.

2.

The most common categories of detected malware were trojans, downloaders, backdoors, spyware, keyloggers and cryptominers.

3.

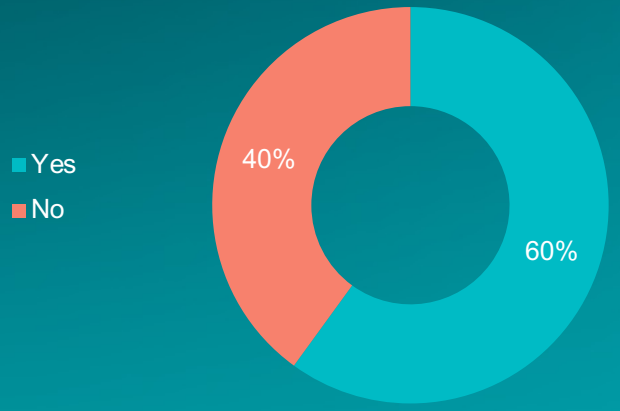
Dozens of skills included social engineering and phishing techniques, both inside the skill itself and in the ecosystem around them.

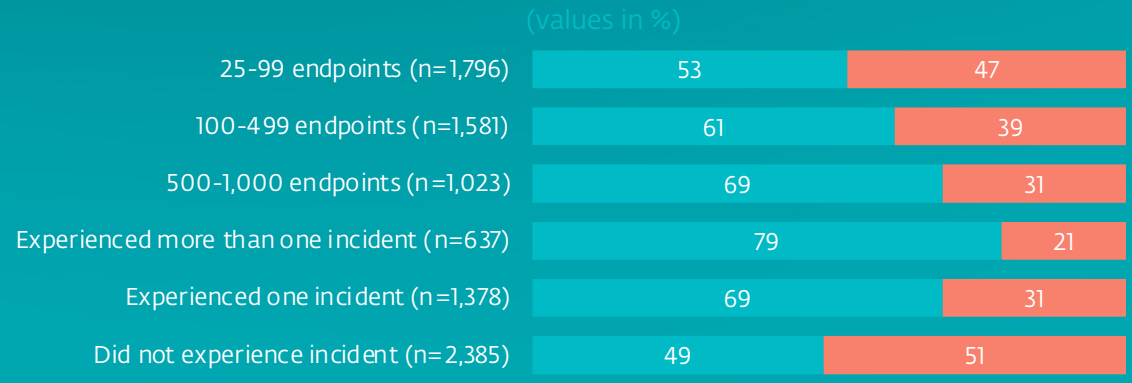
Some SMBs Ignore AI At Their Peril

73% of businesses that don't integrate AI tools also don't have AI policies

- Despite heavy use of AI tools by cybercriminals, many businesses still don't address these threats properly: (40%) of all businesses do not have a proper AI policy.
- The data also revealed that most businesses that don't integrate AI tools also tend to ignore the relevance of AI policies. But employees still use publicly available tools to boost their performance without their managers knowing it.

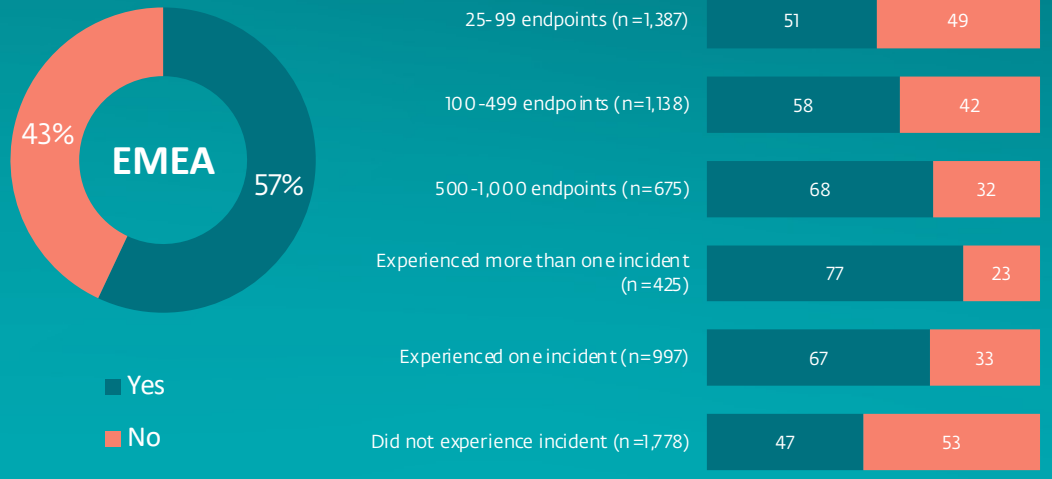
AI policy to restrict use of AI applications outside approved processes or platforms (shadow AI)





Globally, SMBs that experienced more than one incident are much more concerned about the use of shadow AI. NORAM businesses restrict shadow AI more often across all surveyed segments.

AI policy to restrict use of AI applications outside approved processes or platforms (shadow AI)

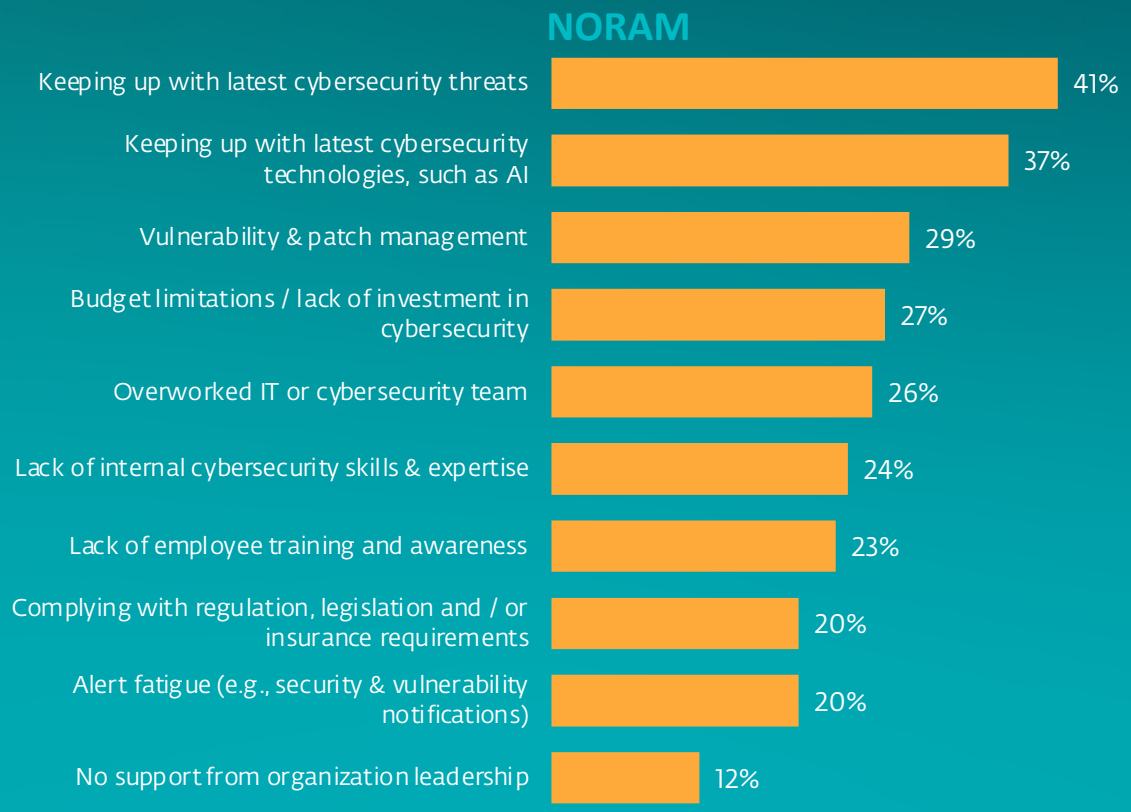


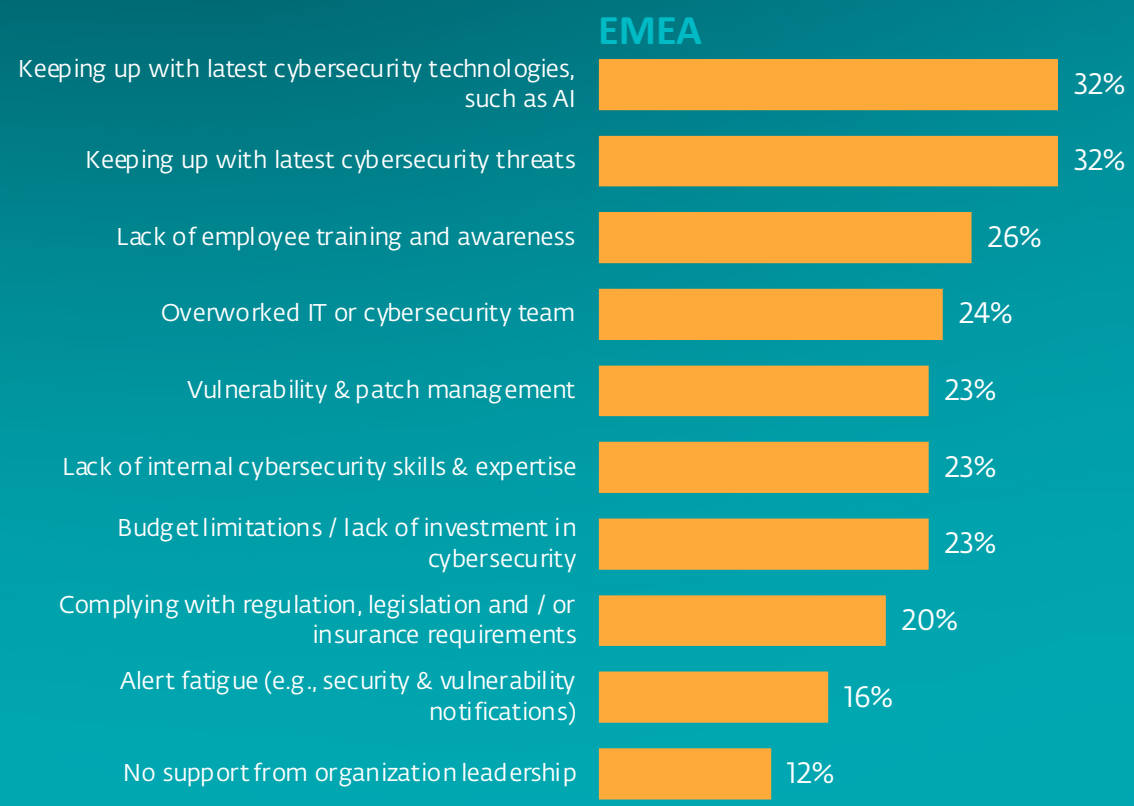
Globally, SMBs Want To Better Understand And Anticipate Attacks. AI Can Help

- The biggest cybersecurity challenge for SMBs? Keeping up with latest cybersecurity threats.
- Second biggest? Keeping up with AI tech to help them do it.
- SMBs see clear utility in AI for cyber defense – but either the tools aren't there yet, or they're not available.
- In comparison with 2022 (43%), SMBs are now much less concerned about their employees not having access to quality cyber awareness training (27%).

The biggest cybersecurity challenges

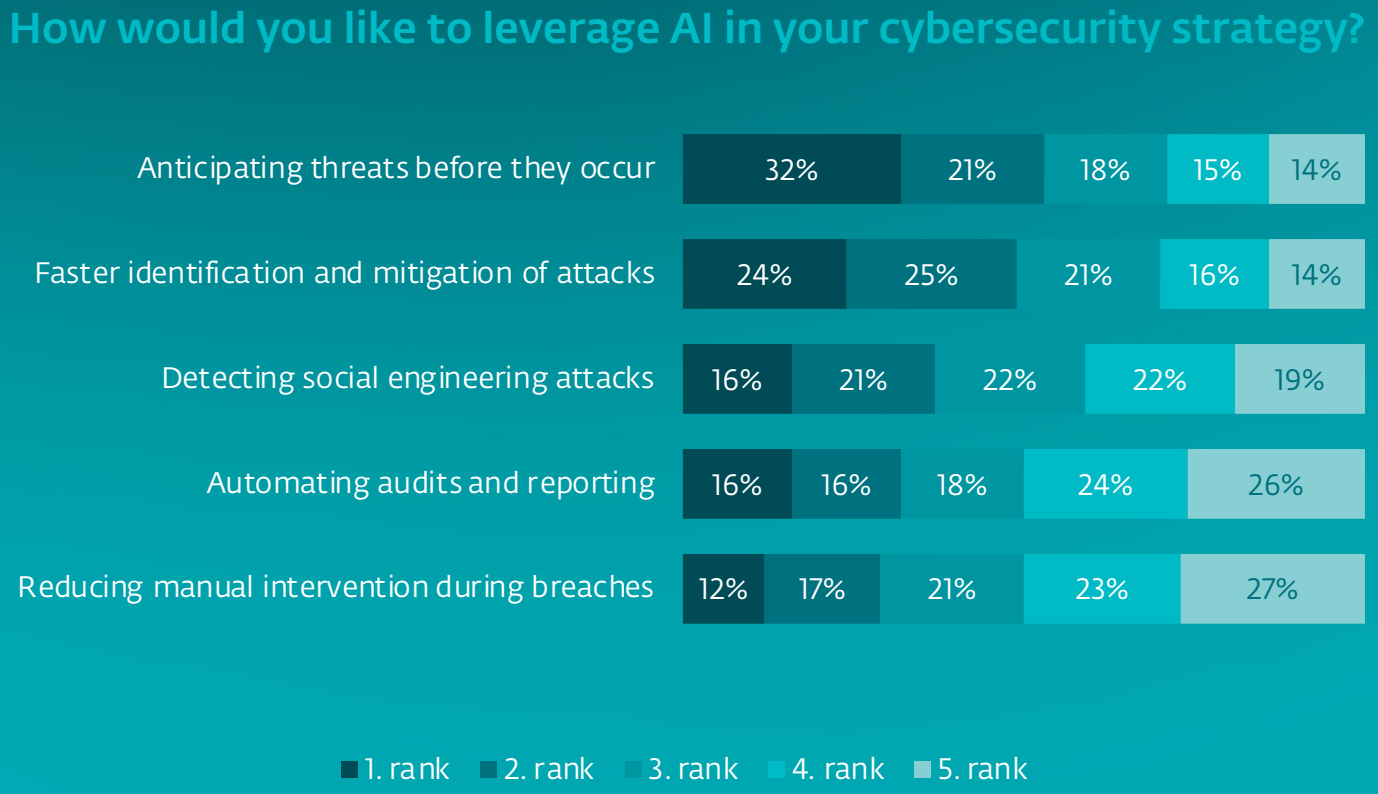
- North American businesses are more concerned about the latest threats and technologies. They also mention alert fatigue more often.
- SMBs in the EMEA region are more worried about their employees' awareness.





Concern Over Threats Vectoring From AI Run In Parallel To Businesses Identifying Its Value For Cybersecurity

- SMBs are overly worried about AI threats, but also keen to harness AI to do more – including improving cybersecurity, specifically prevention and mitigation capabilities.
- SMBs see real value across all options, but automated audits / reports and the idea of AI replacing manual human intervention when dealing with ongoing breaches appear to be the least useful.



4

Budgeting Cybersecurity

Budget-Savvy SMBs Spend Smart

Resources

SMBs face increasingly sophisticated attacks while often juggling budgets that prohibit significant investment and operational spend.

Put simply: SMBs just don't have the same resources on hand to tackle cybersecurity as large enterprises do. So, SMBs have relied on sharp budgeting and outsourcing to managed services.

MDR

The highest and/or most powerful AI-equipped tiers of security solutions may be out of reach, but Managed Detection and Response (MDR) provides defense in-depth and information-rich threat intel on top.

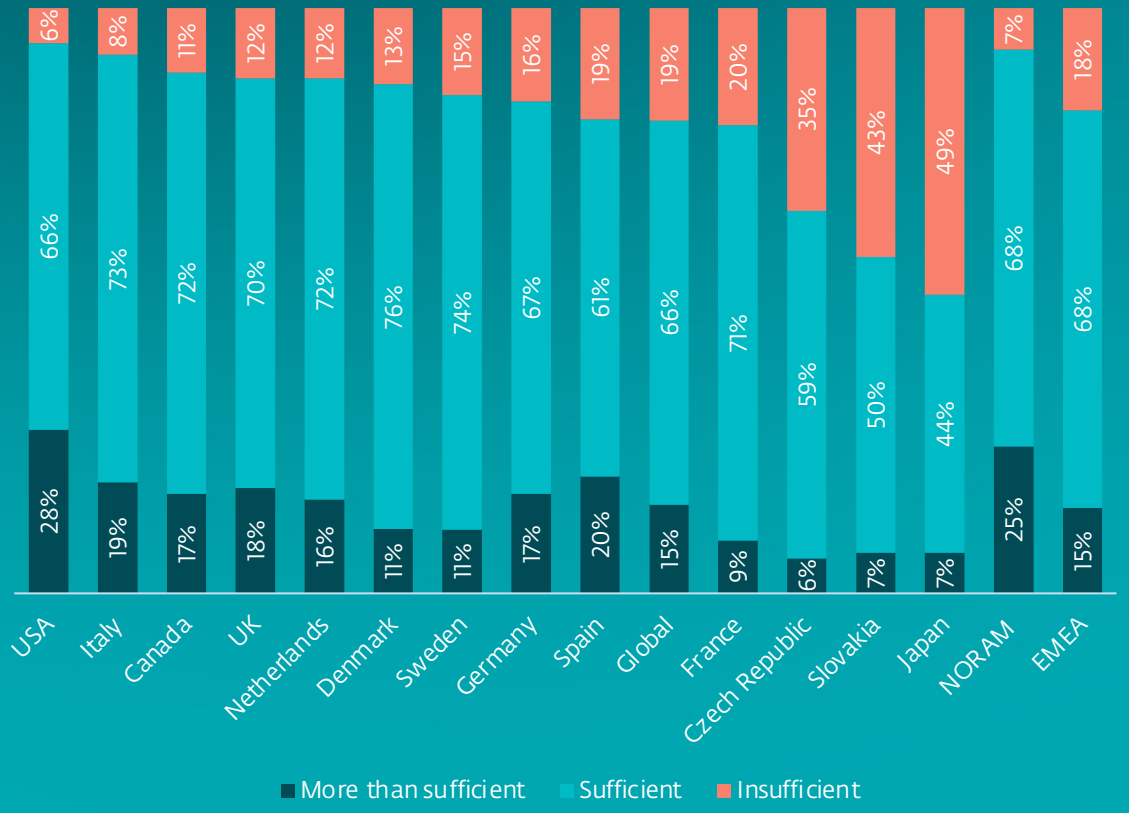
Smart budget

Looking at the data from our panel, SMBs are practicing smart budget planning.

SMB Security Managers Are – Perhaps Surprisingly – Generally Happy With Their Cybersecurity Budgets

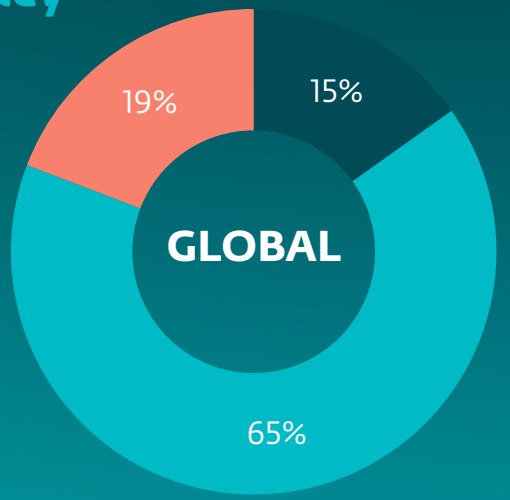
- Cybersecurity leads at SMBs in America, Italy, Canada and the UK seem quite happy with their budgets.
- The majority of respondents describe their budgets as “sufficient” or “more than sufficient”. Only between 6% and 12% of respondents in these countries say their budget is “insufficient”.
- The US also leads in responding “more than sufficient”, where the budget is perceived in this way in 28% of cases. Spain, ranks 2nd in terms of responding “more than sufficient” although it is not among the top places overall.
- Japan registers an interesting outlier because in the context of incident data it ranks high, but simultaneously demonstrates low “confidence” and budget insufficiency.

Cybersecurity budget adequacy



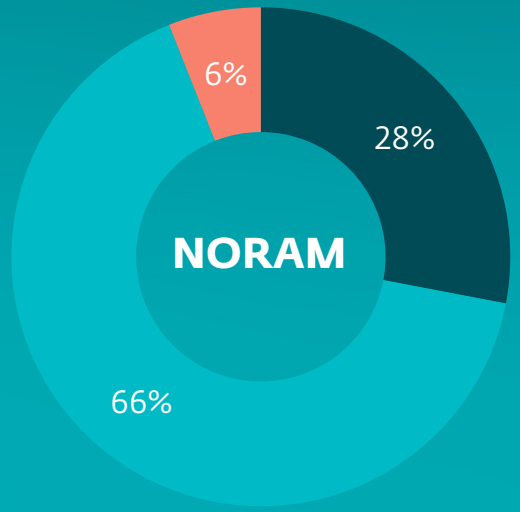
Cybersecurity budget adequacy

- When it comes to expenditures, U.S. businesses seem quite satisfied with their budgets.
- Twice the number of North American SMBs experiencing more than one incident feel that their budget is more than sufficient.



(values in %)

25-99 endpoints (n=1,796)	14	67	19
100-499 endpoints (n=1,581)	15	64	21
500-1,000 endpoints (n=1,023)	18	64	17
Experienced more than one incident (n=637)	29	56	15
Experienced one incident (n=1,378)	15	67	17
Did not experience incident (n=2,385)	12	66	22



(values in %)

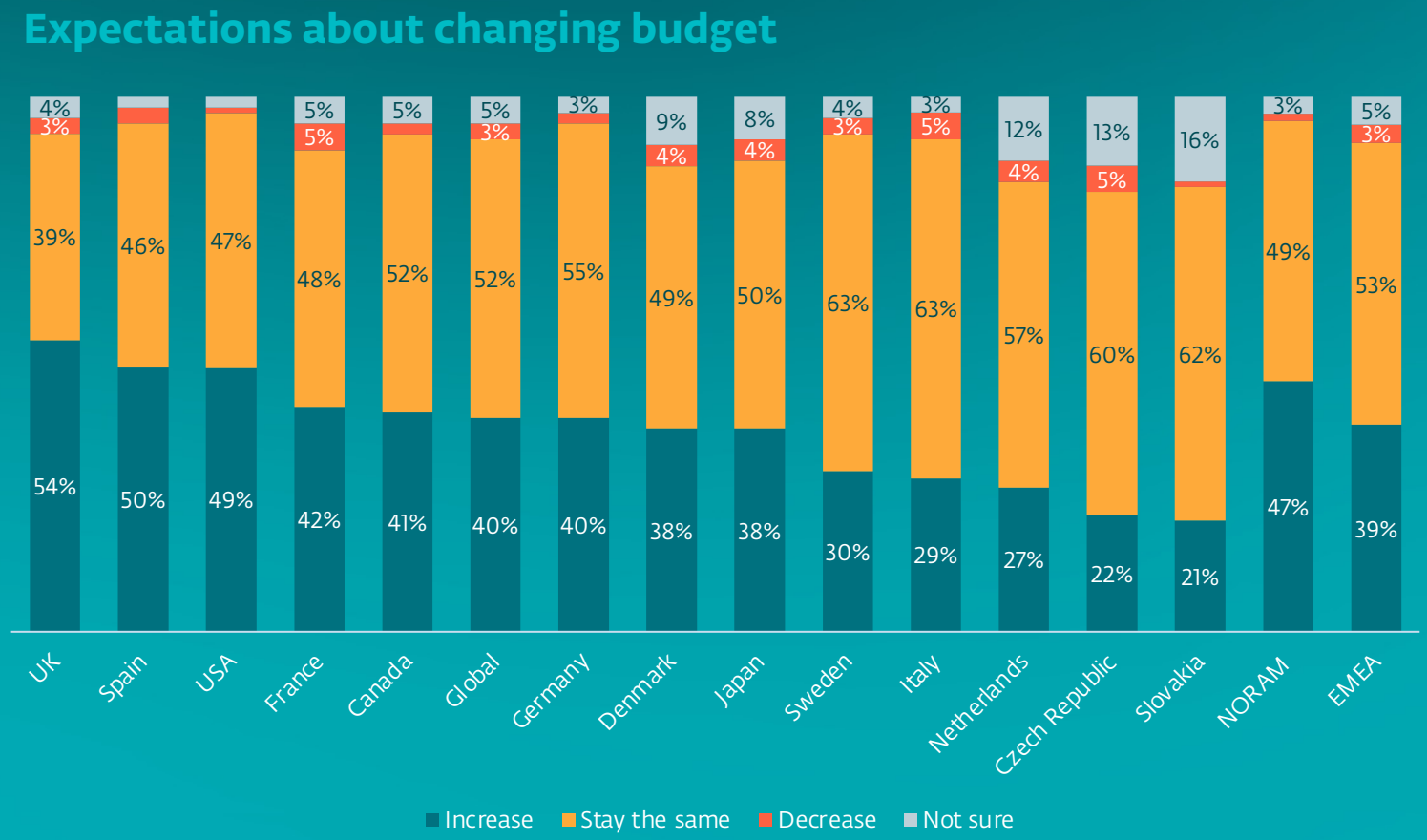
25-99 endpoints (n=257)	25	68	6
100-499 endpoints (n=260)	30	65	4
500-1,000 endpoints (n=183)	30	63	6
Experienced more than one incident (n=133)	45	54	
Experienced one incident (n=225)	23	70	6
Did not experience incident (n=342)	24	69	7

More than sufficient
Sufficient
Insufficient

Great Expectations? SMBs Are Relaxed About Cybersecurity Budget Increases

- On one hand, an overall decrease in budget for cybersecurity is not expected by respondents. On the other, an increase in budget is expected more often in countries that already have high current budget sufficiency including the UK, Spain, the US and Canada.

- Globally, 40% of respondents expect an increase in the budget (this trend is also visible for both Germany and Japan).

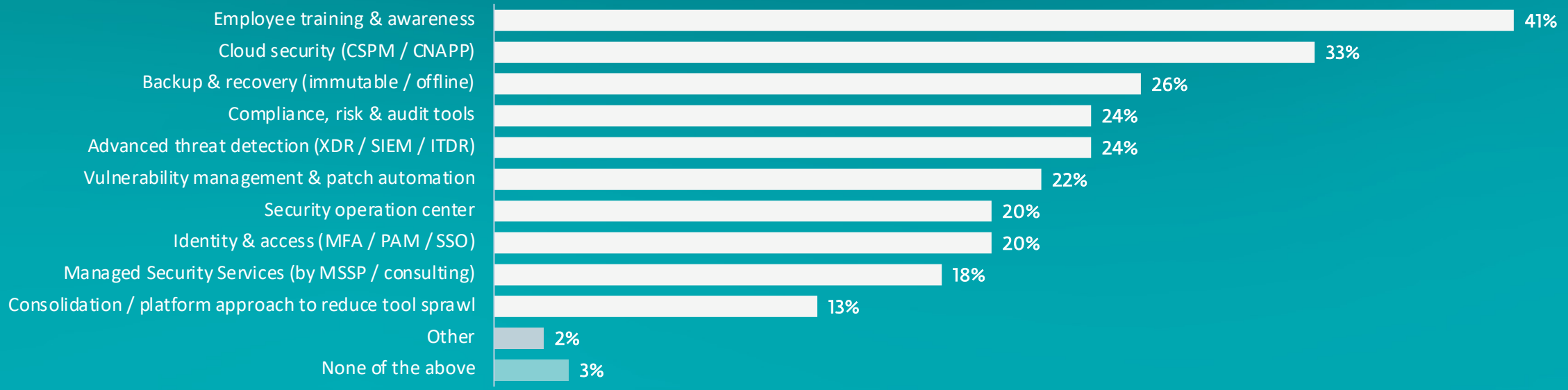


Budgeting For Cyber Resilience In The AI Era

When credible phishing emails can be generated in seconds and deepfakes are almost unrecognizable from reality, cybersecurity awareness becomes more important than ever.

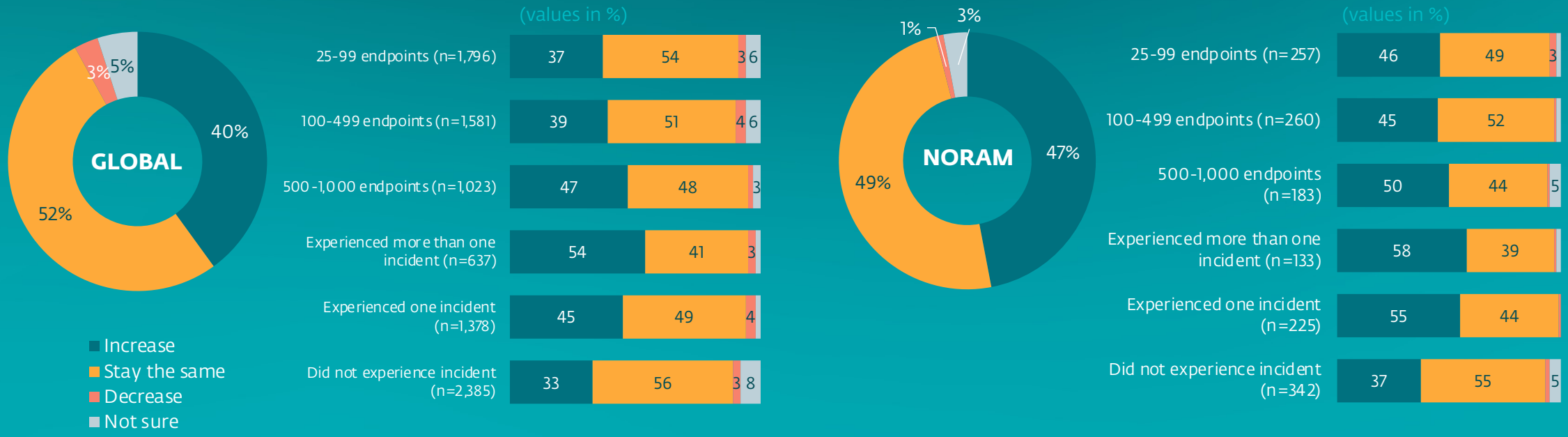
As cyberattacks grow in sophistication, SMBs also need advanced cybersecurity solutions such as XDR, cloud security, or threat detection tools to face the latest tactics and malware.

Planned investments in next 12 months



More North American Businesses (47%) Expect A Budget Increase In Future. Globally, Budget Expectations Are Slightly Lower.

Expectation about changing budget

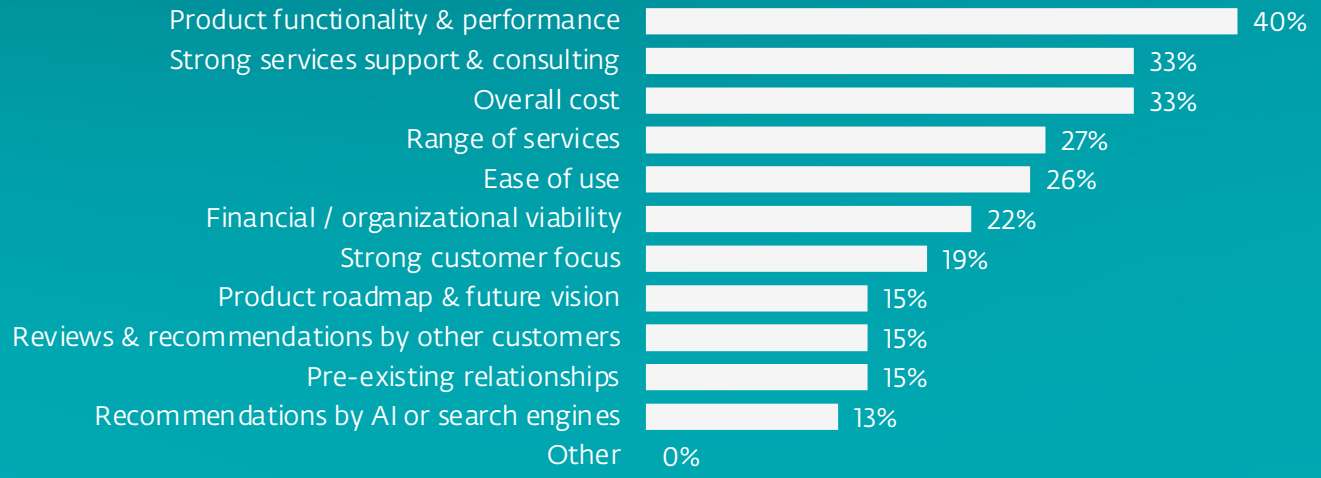


Budget Is Still The Top Barrier, Followed By Complexity And Speed

- Nearly one in four SMBs feel that an increased budget would help them improve their cybersecurity at a faster rate.
- Among the biggest challenges are also complexity and integration – a common problem for businesses trying to manage cybersecurity on their own.
- This aligns with respondents' cybersecurity preferences: SMBs seek reliable, feature-rich services and solutions, and easy-to-use protection.

Current barriers to improve cybersecurity in the company

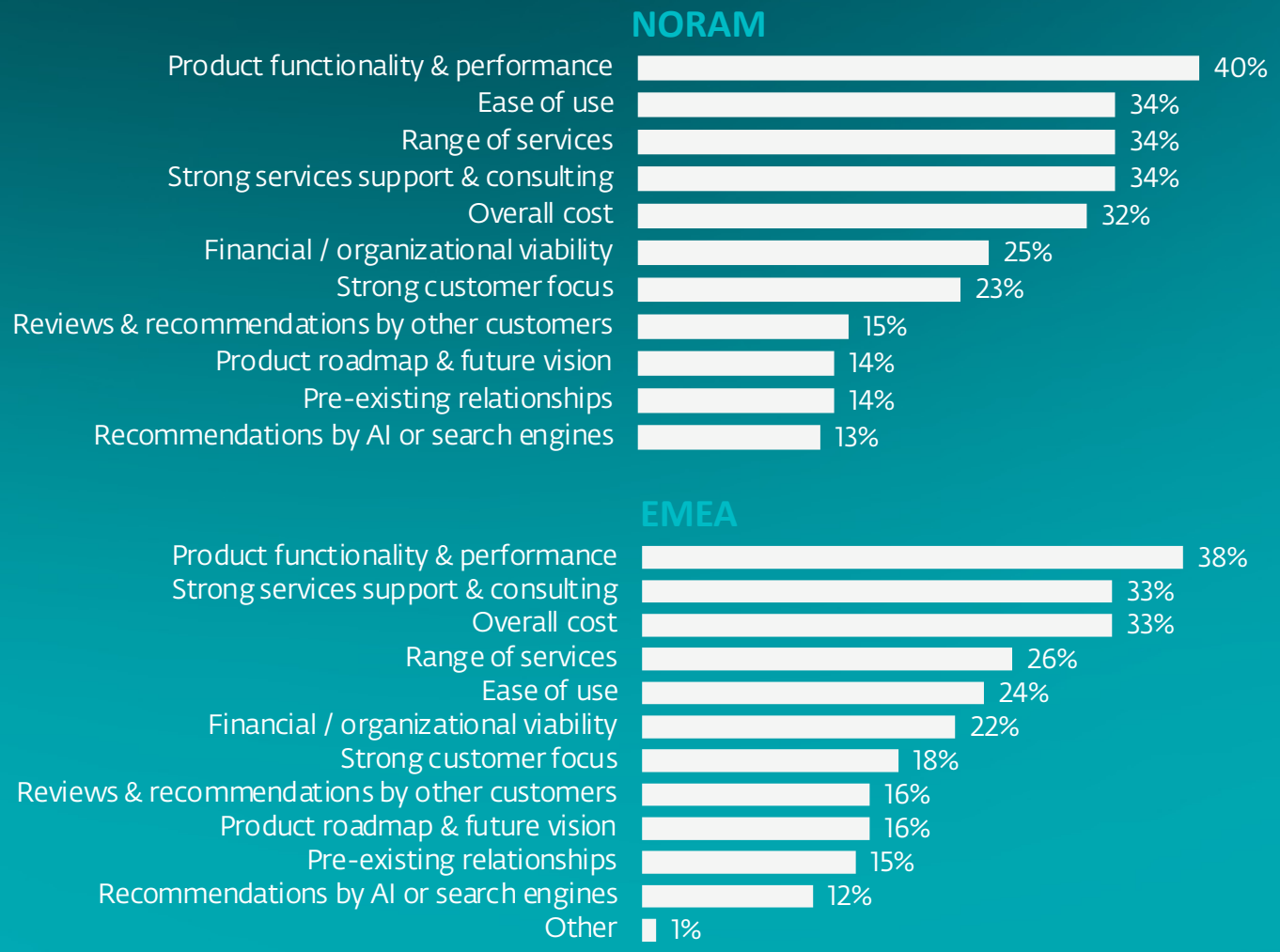
The most important factors in terms of choosing cybersecurity solutions



For North American Businesses, Ease Of Use Is A Key Factor

- The majority of surveyed SMBs choose their cybersecurity solution based on product performance, support and overall cost.
- Businesses in the North American region place more emphasis on ease of use, the range of services and strong customer focus.

The most important factors in terms of choosing cybersecurity solutions



5

SMBs Are Investing In Security

SMBs Are Investing in Security

The Good News

Small and medium-sized businesses are investing; they aren't waiting to be attacked. They're turning to cyber insurance as the impact of incidents becomes both real and inevitable.

They're investing in training, too. Combined, these forces are causing SMB cyber resilience to show real signs of growth.

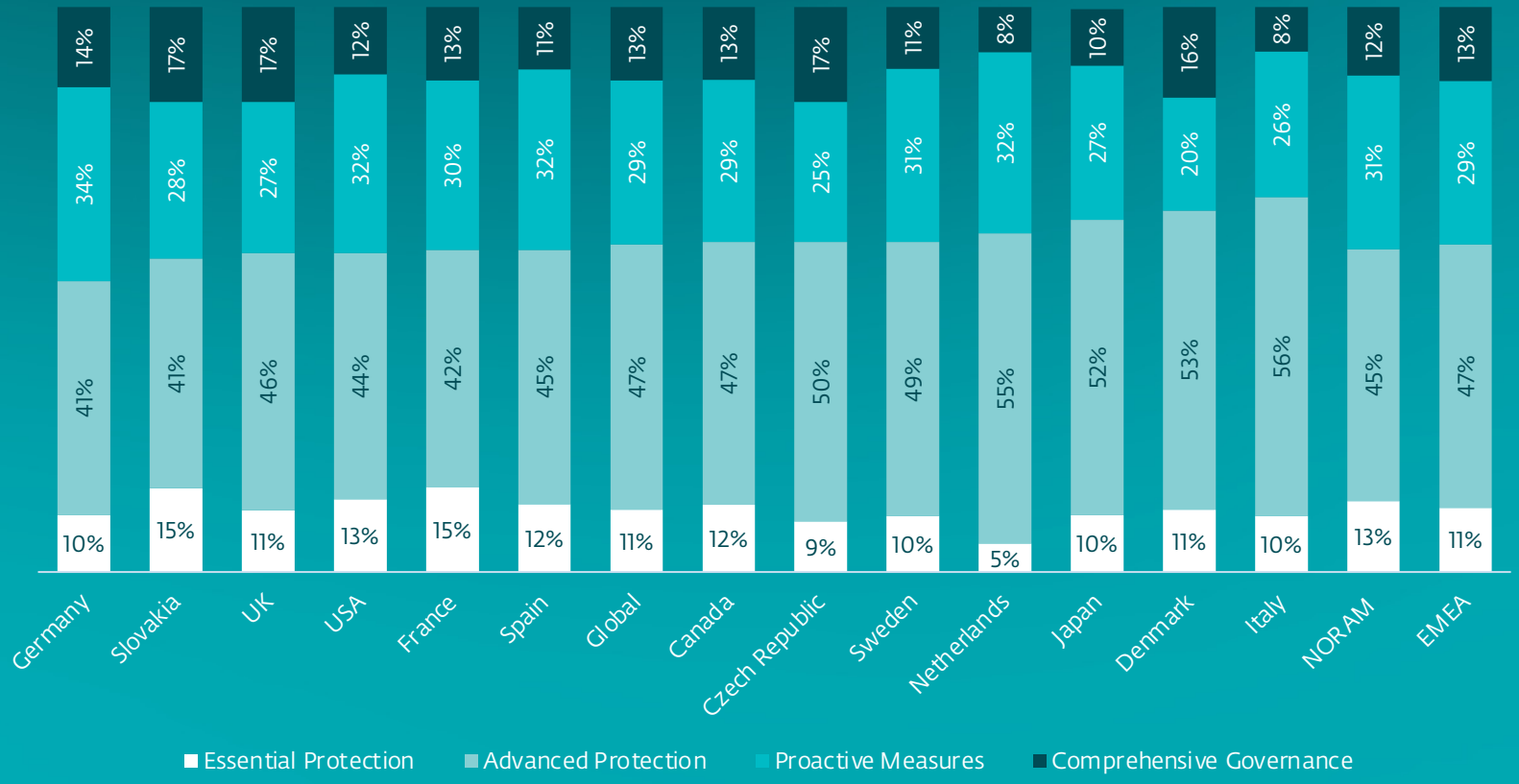
Diversified outsourcing models

For those organizations that outsource, managed security services are critical – and come via several different routes. It can be driven by the use of insurers and, in some cases, past record of security incidents.

Small And Midsize Businesses Take Their Security Seriously

- Cybersecurity posture is quite diverse across the globe, although, naturally, the middle tiers are preferred the most.
- The highest tiers of cybersecurity are most often sought in Germany, followed by Slovakia, the UK, and the US. At the same time, the US, together with France, Slovakia and Spain prefer essential tiers of cybersecurity.

Cybersecurity posture



- Looking at particular SMB segments, we can see that smaller companies and businesses that have experienced multiple incidents are slightly more often protected by lower tiers of cybersecurity.
- Naturally, larger companies with more resources more often go for higher tiers.

Cybersecurity posture

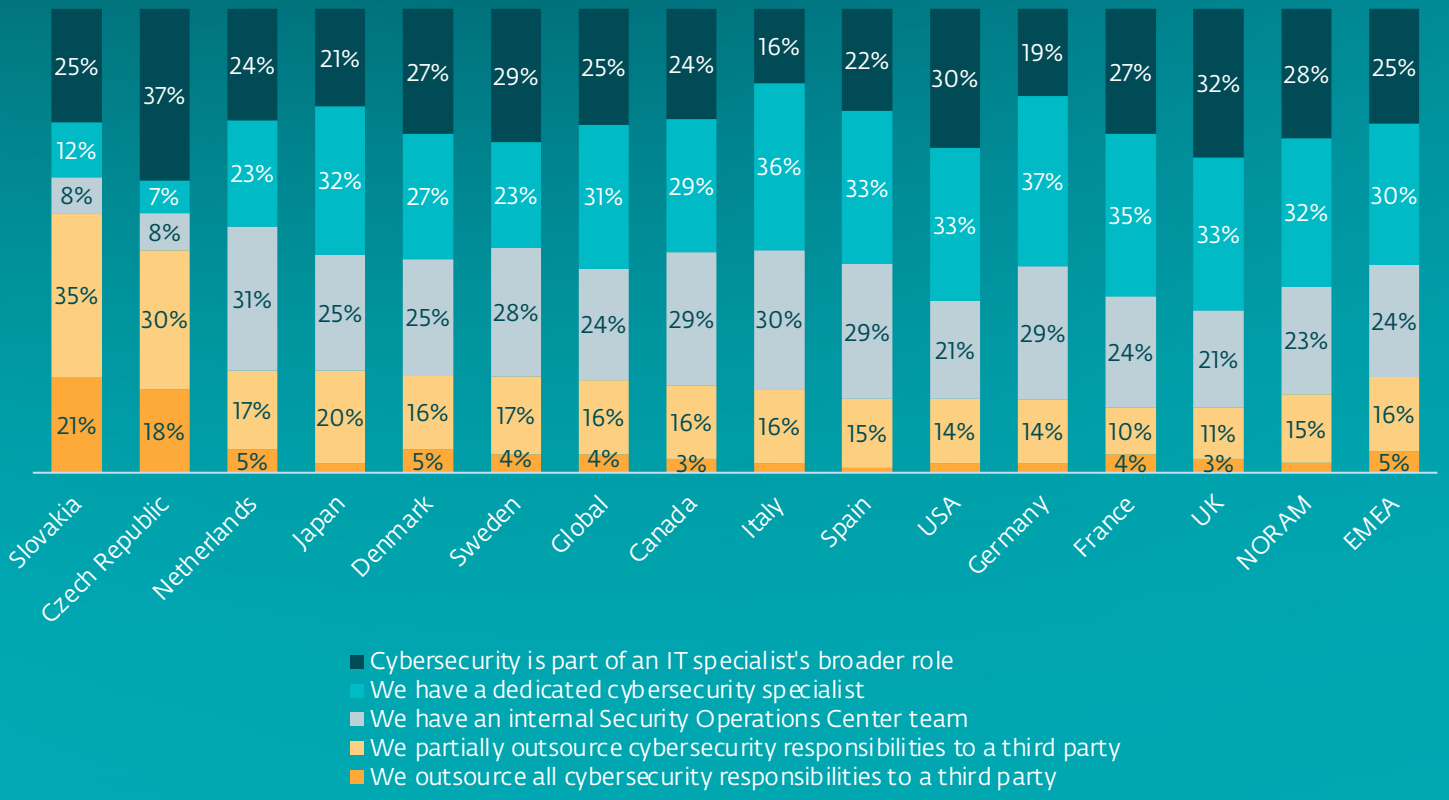
(values in %)

25-99 endpoints (n=1,796)	12	49	29	11
100-499 endpoints (n=1,581)	10	47	30	13
500-1,000 endpoints (n=1,023)	13	44	28	15
Experienced more than one incident (n=637)	17	45	26	12
Experienced one incident (n=1,378)	11	48	29	12
Did not experience incident (n=2,385)	10	47	30	13

SMB Outsourcing VS DIY: Many Prefer To Handle Cybersecurity In-House – With Two Big Exceptions

- Most businesses across all surveyed regions have their own cybersecurity management.
- In terms of "specialized internal capacities", i.e., the "Dedicated cybersecurity specialist" & "internal SOC" options, Italy leads, followed by Germany, Spain, France, Canada and Japan.
- The US and the UK are somewhere in the middle in this regard, both in terms of partial & full outsourcing, internal capacity and IT generalists.
- Slovakia and the Czech Republic are outliers regarding outsourcing in general.

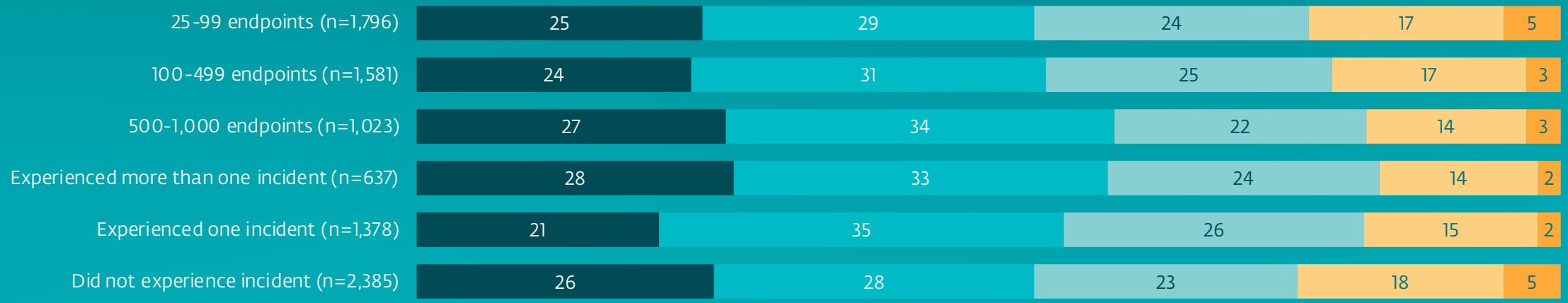
Managing cybersecurity in the company



Managing cybersecurity in the company

- 96% of companies surveyed said they have fully or partially realized cybersecurity responsibilities in place, with around 25% fully controlled by general IT specialists.
- Interestingly, smaller businesses and those which did not experience an incident outsource their cybersecurity more often.

(values in %)

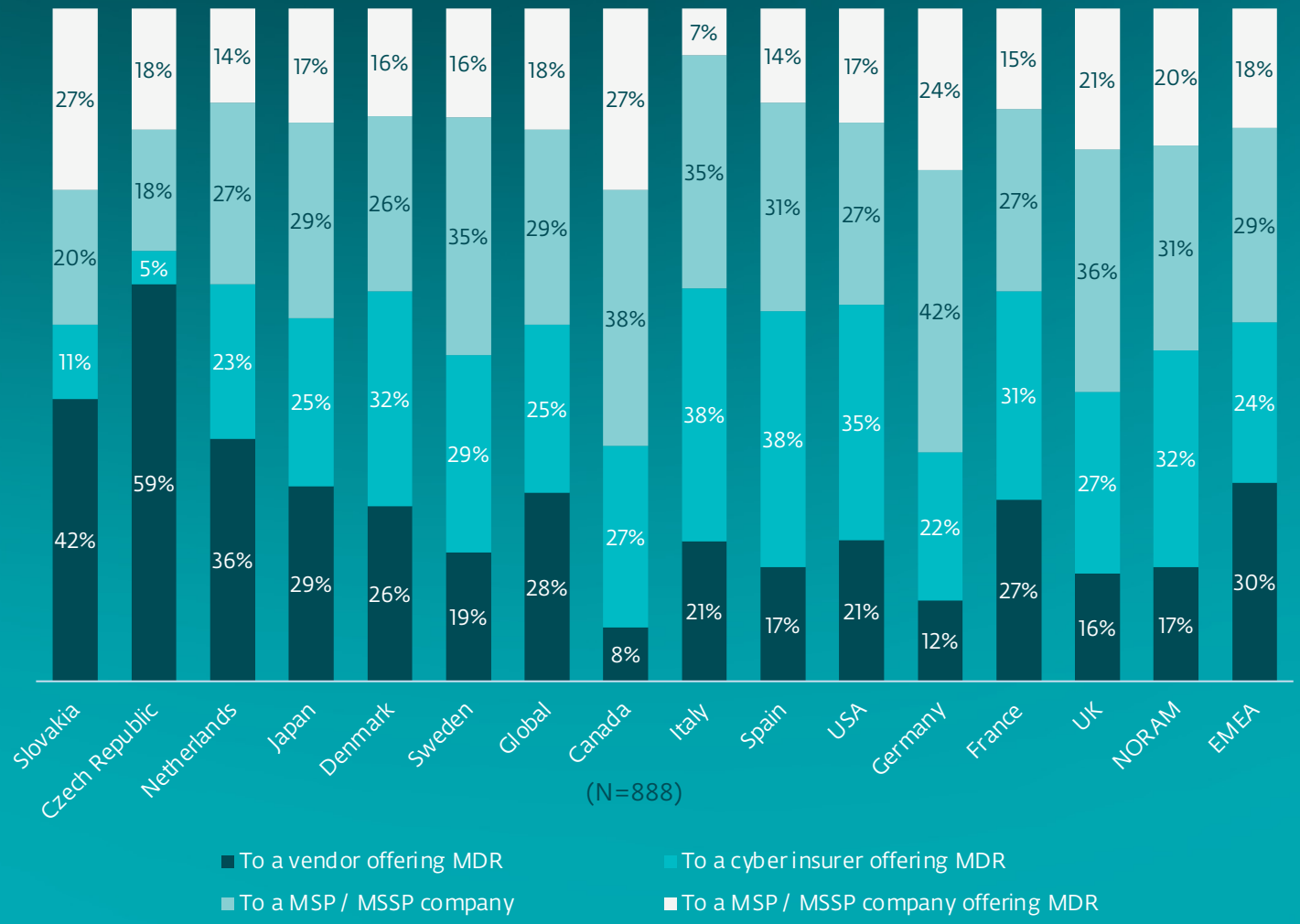


MDR Hits The Mainstream

- Approaches to outsourcing vary from country to country. Czech and Slovak businesses prefer vendors offering MDR. Italy, Spain and the US prefer cyber insurers offering MDR or MSPs/MSSPs with MDR. Canada, Germany and UK tend to have MSPs/MSSPs with or without MDR.

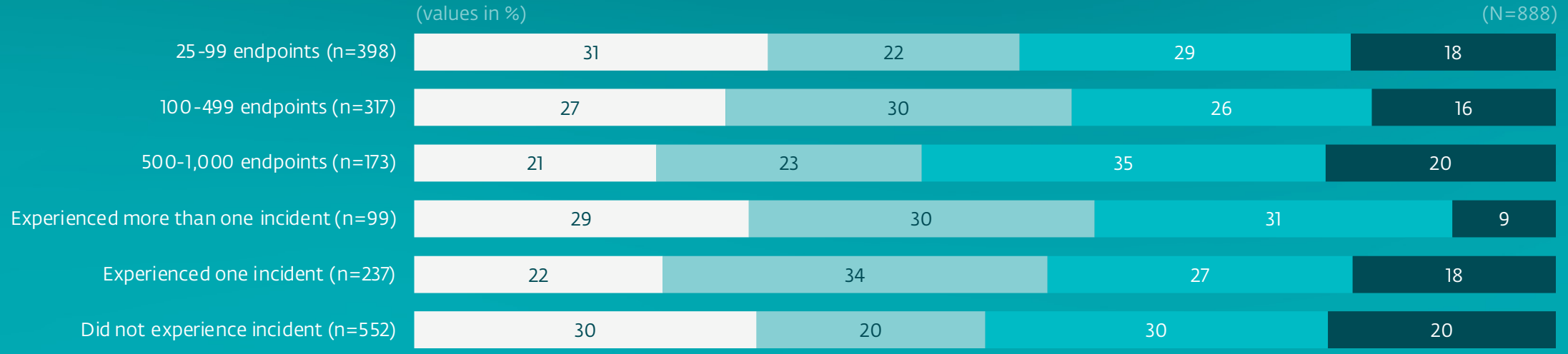
- Countries including Germany, Italy and Spain, which responded that they have better internal capacities (Specialists or SOC), outsource via cyber insurance or MSP/MSSP and less so via vendors.

The way of outsourcing cybersecurity services



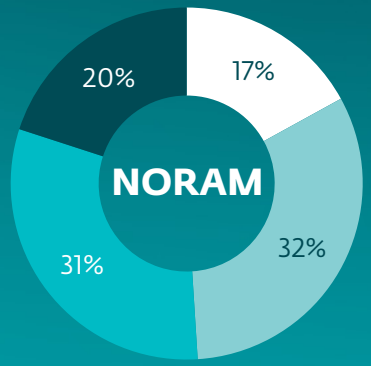
- Globally, SMBs choosing to outsource equally select vendors with MDR, cyber insurers with MDR and MSPs/MSSPs without MDR. MSPs/MSSPs offering MDR are the least favorable option.
- MSPs/MSSPs (with or without MDR) are more popular among bigger companies and those that did not experience cyber incident.

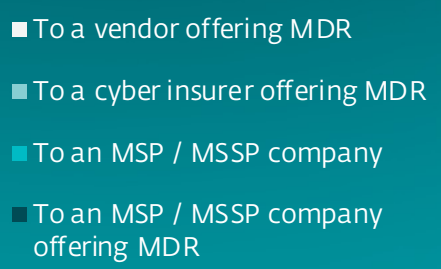
The way of outsourcing cybersecurity services

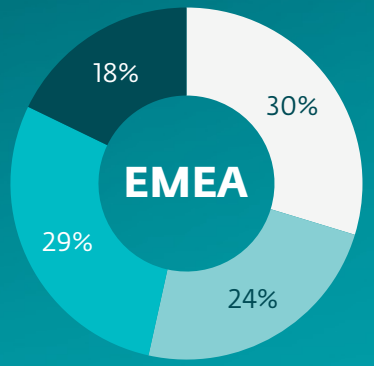


- In North America, SMBs with 100-499 endpoints and those with incident experience prefer insurers as MDR providers.
- Among SMBs in EMEA, the most popular option is security vendors offering MDR. This is notable amongst SMBs with 25-99 endpoints and those with 100-499 endpoints and those who did not experience an incident.

The way of outsourcing cybersecurity services







(values in %)

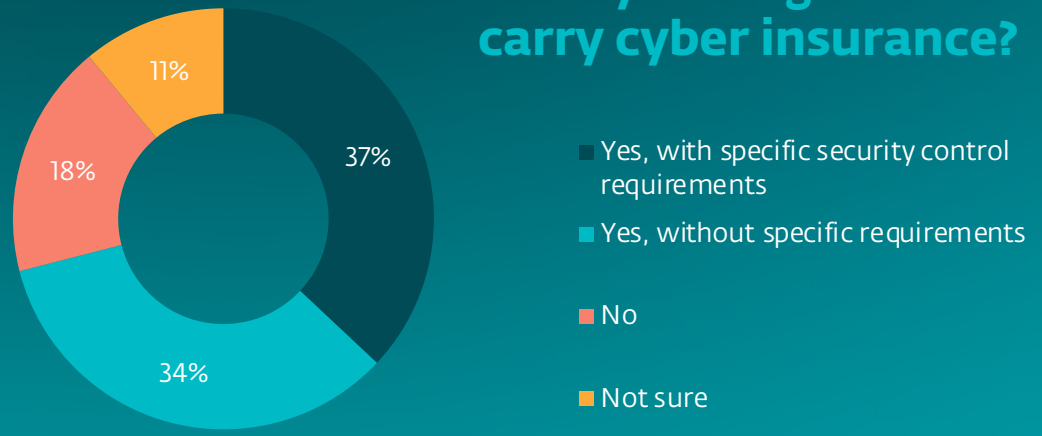
	To a vendor offering MDR	To a cyber insurer offering MDR	To an MSP / MSSP company	To an MSP / MSSP company offering MDR
25-99 endpoints (n=43)	28	33	21	19
100-499 endpoints (n=45)	7	42	33	18
500-1,000 endpoints (n=30)	17	17	40	27
Experienced more than one incident (n=20) *	20	45	25	10
Experienced one incident (n=35)	14	34	20	31
Did not experience incident (n=63)	17	27	38	17

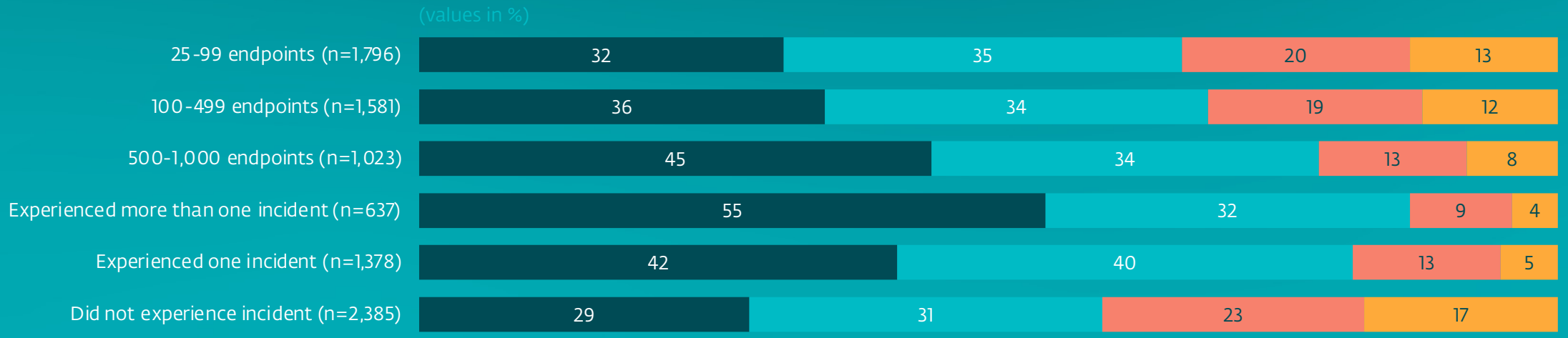
(values in %)

	To a vendor offering MDR	To a cyber insurer offering MDR	To an MSP / MSSP company	To an MSP / MSSP company offering MDR
25-99 endpoints (n=322)	31	19	31	19
100-499 endpoints (n=226)	33	29	23	15
500-1,000 endpoints (n=112)	19	26	35	21
Experienced more than one incident (n=70)	30	27	33	10
Experienced one incident (n=171)	23	35	27	15
Did not experience incident (n=419)	32	19	29	20

Cyber Insurers Step In

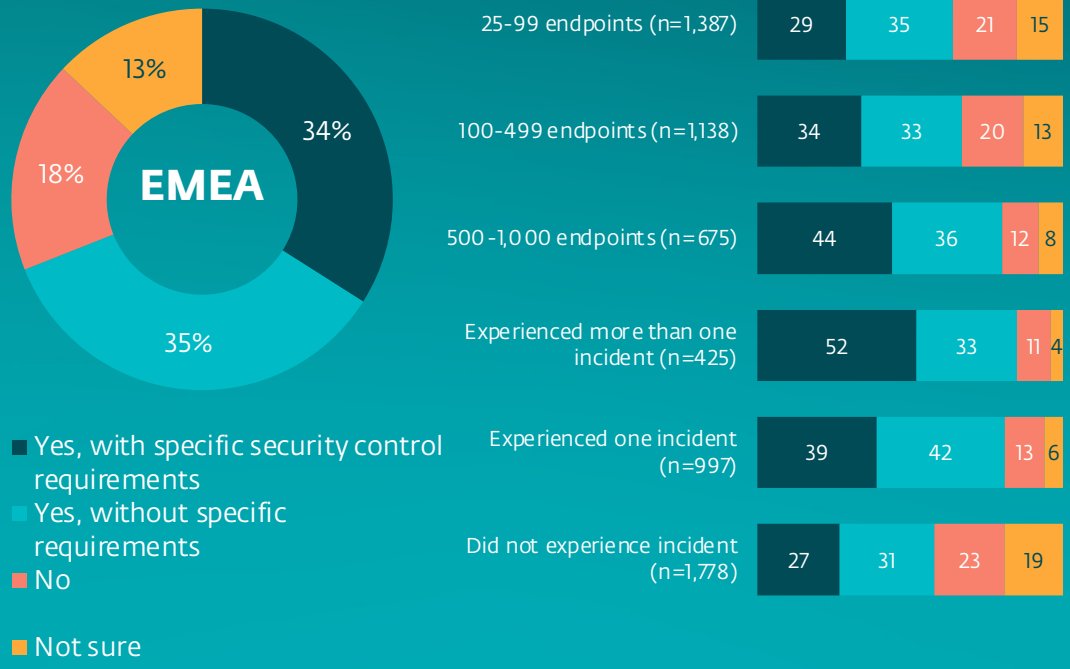
- Resource-constrained SMBs are turning to insurance in order to offset risks. 84% of North American SMBs carry cyber insurance, 51% of which include specific security control requirements.
- In the rest of the world, a greater portion of businesses have cyber insurance with less/no specific requirements or no cyber insurance at all.

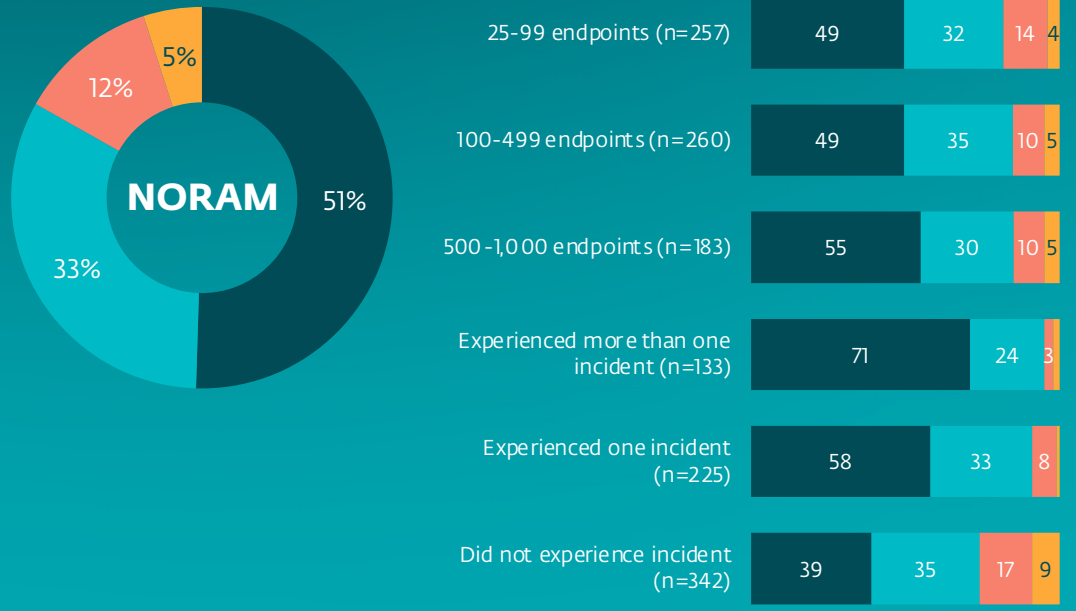




For many SMBs across the globe, having a cyber insurance policy coincides with experiencing an incident, with greater numbers of incidents resulting in having an insurance policy with more specific requirements.

Does your organization carry cyber insurance?

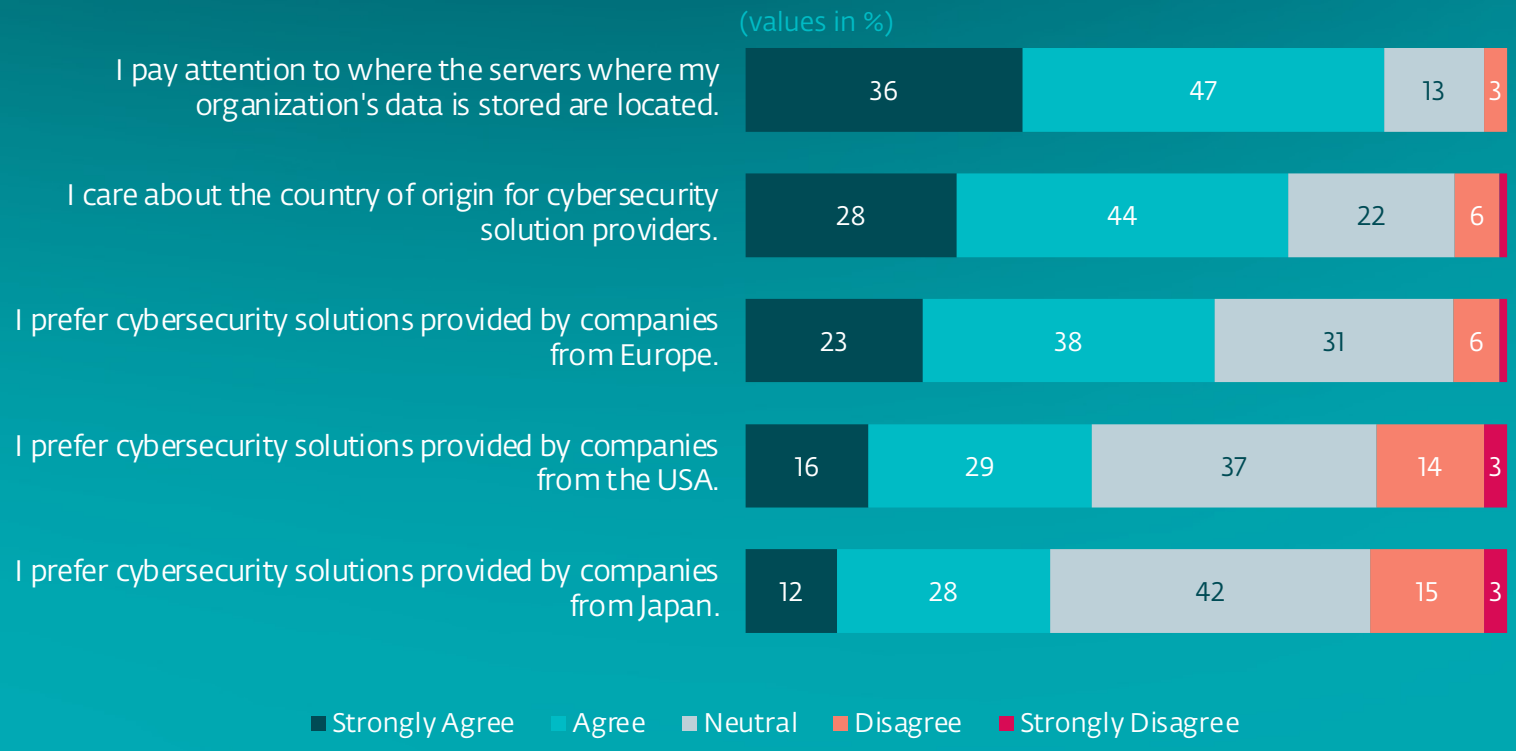




Provider's Country Of Origin Matters To SMBs

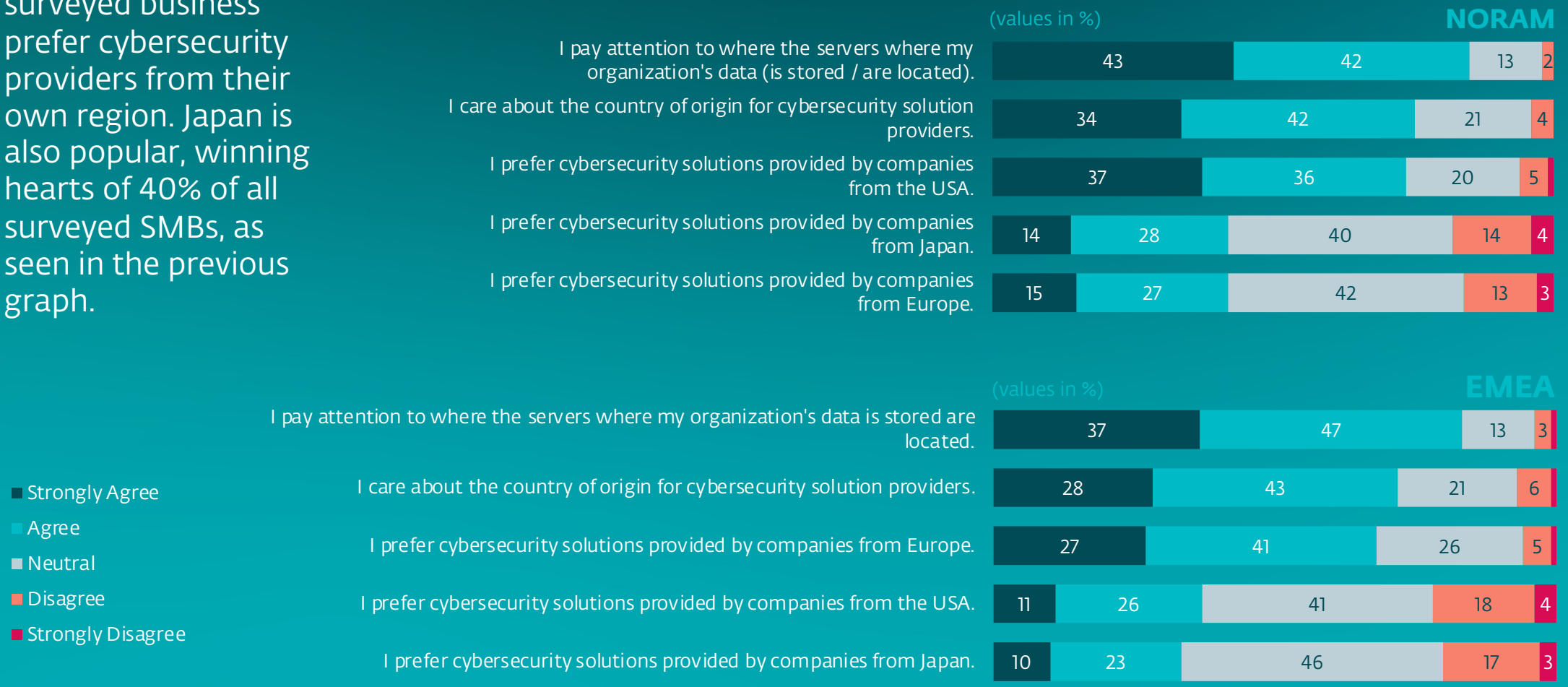
- SMBs across the globe consider their security provider's country of origin, and server location, as important factors when choosing cybersecurity solutions.
- Overall, Europe is ranked as the most preferred region in this report, likely linked to the sample structure, where 700 surveyed businesses were located in NORAM and 3,200 SMBs come from across the EMEA region.

To what extent do you agree with the following statements?



These graphs show that around 70% of all surveyed business prefer cybersecurity providers from their own region. Japan is also popular, winning hearts of 40% of all surveyed SMBs, as seen in the previous graph.

To what extent do you agree with the following statements?



6

Businesses Take Cybersecurity Awareness Training Seriously

Businesses Invest In Cybersecurity Awareness Training

Confidence

The high level of confidence among surveyed businesses concerning their ability to handle phishing and social engineering likely stems from their investment in cybersecurity awareness programs.

Awareness

While many businesses detect phishing attempts as incidents, these often do not escalate into breaches or cause tangible harm thanks, in part, to trained employees.

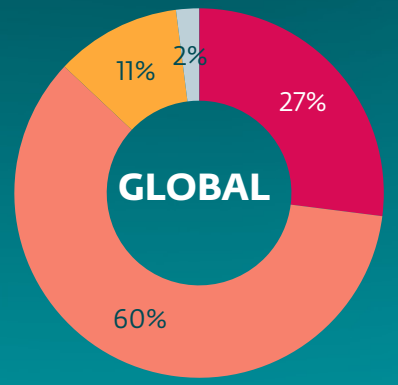
Training

While buying (or renting) technology will solve part of the cybersecurity puzzle, it is nothing without employees who are trained and know to look out for danger. It's often the first, and best line of defense.

Does Building Resilience Require An Incident?

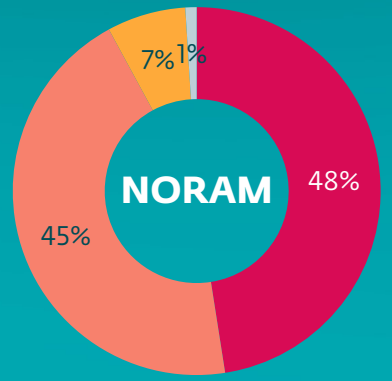
- Those businesses that experienced more than one incident take cybersecurity training more seriously than others, confirming the fact that the human element is often present in incidents and breaches.
- SMBs in North America consider cybersecurity training and awareness critical at a higher rate than the global average.
- When it comes to training, North American businesses across all segments see cybersecurity training as a critical component of cybersecurity.

Importance of cybersecurity training and awareness in preventing attacks



(values in %)

	Critical	Very important	Moderately important
25-99 endpoints (n=1,796)	25	61	13
100-499 endpoints (n=1,581)	28	60	10
500-1,000 endpoints (n=1,023)	31	58	9
Experienced more than one incident (n=637)	30	64	5
Experienced one incident (n=1,378)	27	60	12
Did not experience incident (n=2,385)	27	59	12



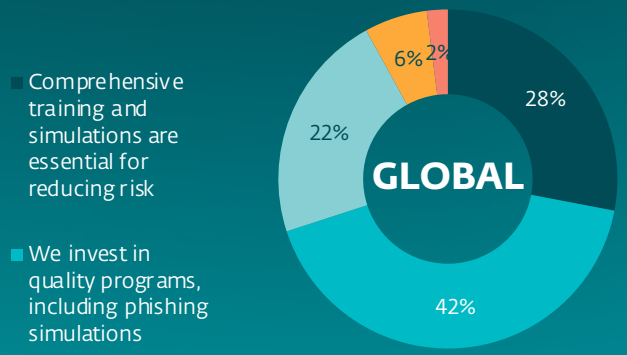
(values in %)

	Critical	Very important	Moderately important
25-99 endpoints (n=257)	48	42	9
100-499 endpoints (n=260)	49	45	5
500-1000 endpoints (n=183)	45	48	6
Experienced more than one incident (n=133)	30	65	4
Experienced one incident (n=225)	46	46	8
Did not experience incident (n=342)	56	36	8

NORAM SMBs Opt For The Highest Tiers Of Security Training More Often Than SMBs Do Globally

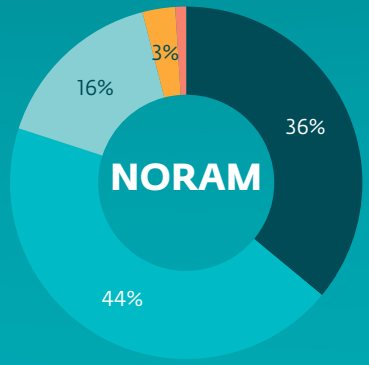
- North American SMBs' view on the importance of training and awareness is reflected in their adoption of higher tiers of training programs – significantly exceeding the global results.
- Only where SMBs responded that they had experienced more than one security incident did North American SMBs (32%) fall behind the global results (35%) in choosing "comprehensive training & simulations".
- Where "quality programs" were deployed, North American SMBs fell short where they experienced a single security incident (42% vs 45%).

Training and awareness situation in organization



(values in %)

25-99 endpoints (n=1,796)	25	41	25	7	
100-499 endpoints (n=1,581)	27	43	22	6	
500-1,000 endpoints (n=1,023)	35	44	17	3	
Experienced more than one incident (n=637)	35	46	15	3	
Experienced one incident (n=1,378)	27	45	21	5	
Did not experience incident (n=2,385)	26	39	25	6	

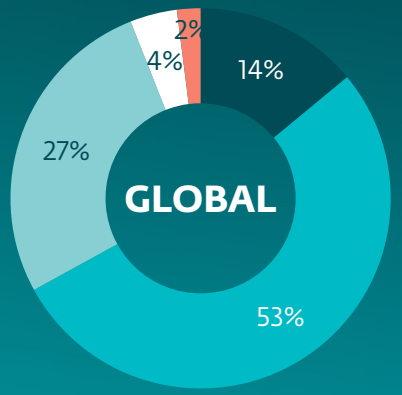


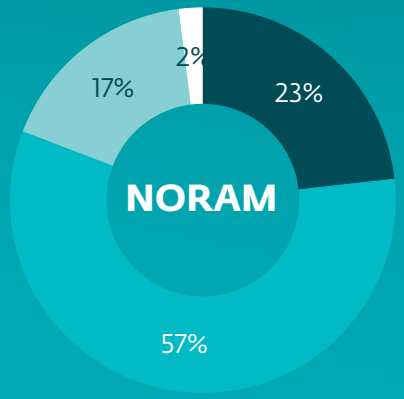
(values in %)

25-99 endpoints (n=257)	30	47	20	2	
100-499 endpoints (n=260)	38	45	13	2	
500-1,000 endpoints (n=183)	42	39	15	4	
Experienced more than one incident (n=133)	32	51	12	4	
Experienced one incident (n=225)	36	42	18	3	
Did not experience incident (n=342)	37	44	17	2	

Practice Makes Perfect... Or At Least More Secure

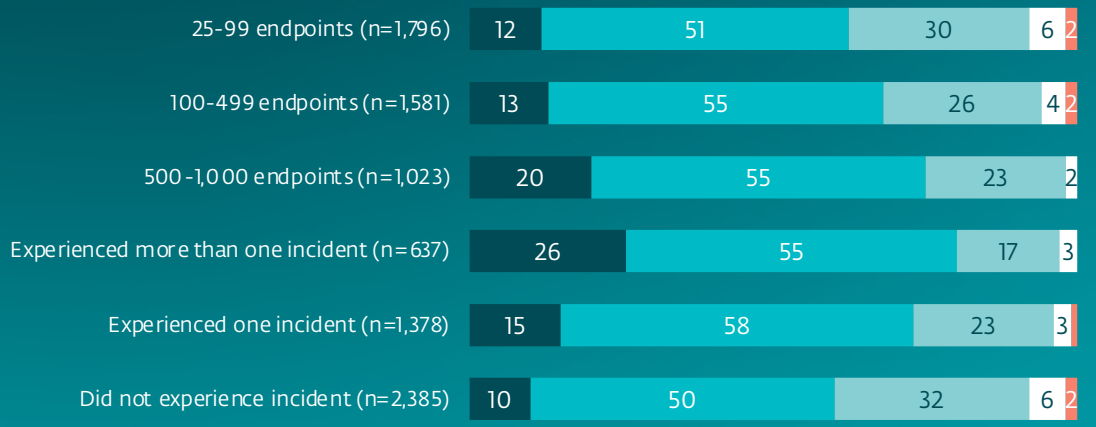
- As expected, North American SMBs also train at a higher cadence than the rest of surveyed countries.
- In particular, those SMBs that experienced multiple incidents in the previous year and larger organizations, train on a regular basis.





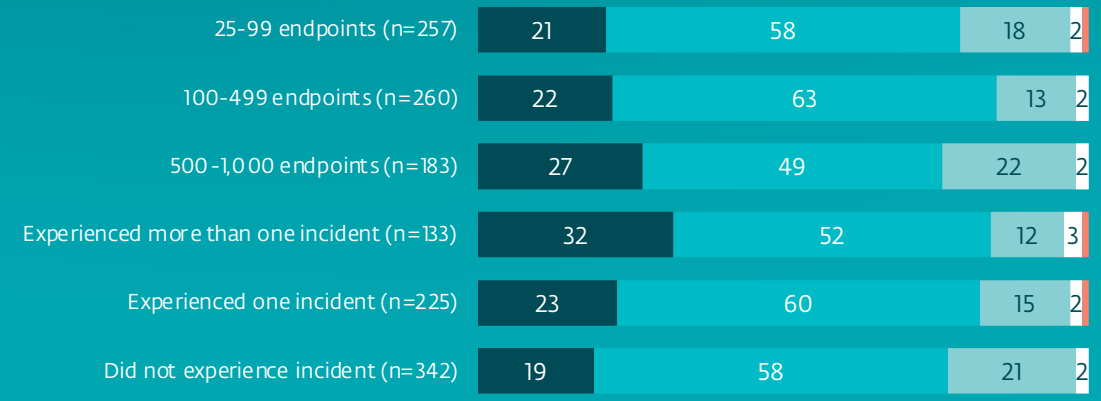
Frequency of cybersecurity trainings in companies

(values in %)



At least once a month | Several times a year | At least once a year | Once every few years | Never

(values in %)



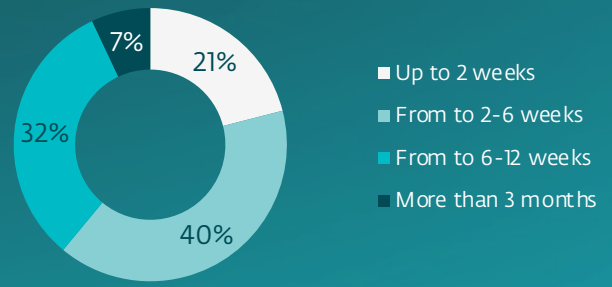
7

Incident Response Has Improved

Incident Investigation Time Has Shortened In Last Four Years

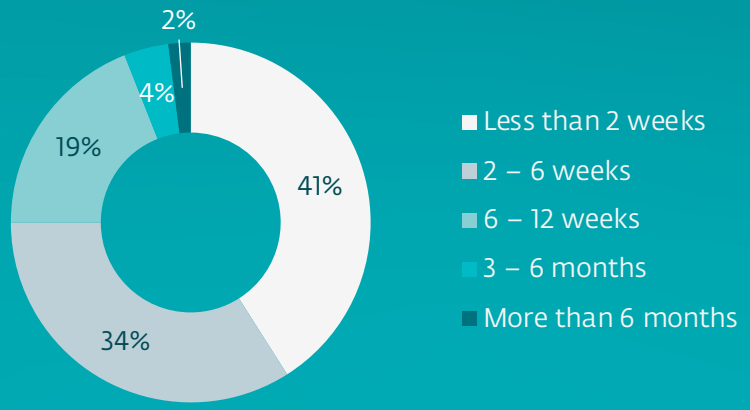
In 2022, the majority of surveyed SMBs needed months to investigate an incident. Four years later, the numbers have improved dramatically, which could be a factor contributing to globally high confidence among SMBs in their cyber resilience.

Incident investigation time globally in 2022

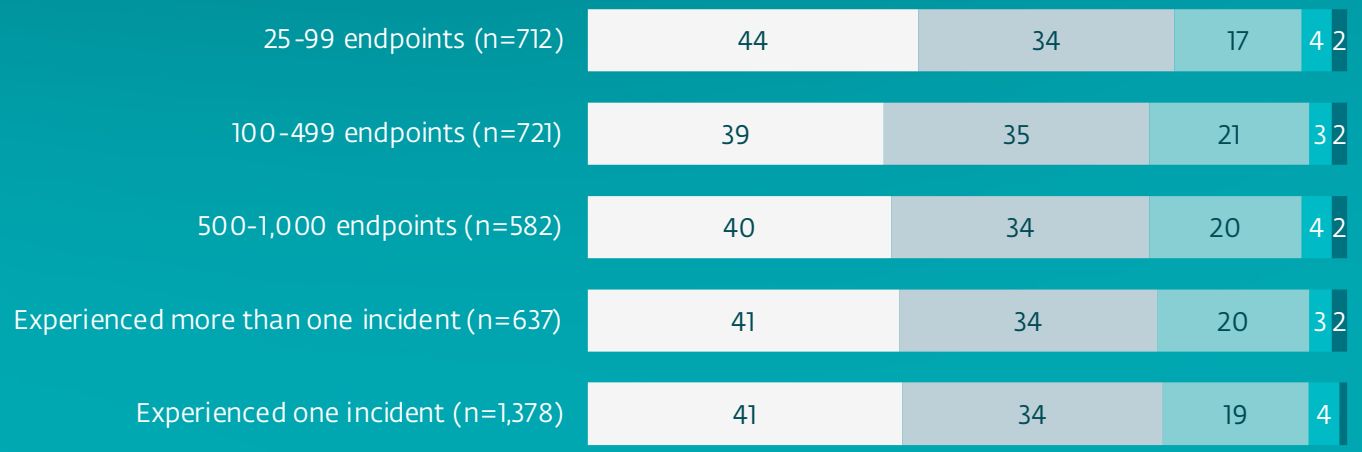


*Note - The 2022 survey did not include Japan (Poland featured instead). Also, the sample size in 2022 was 838 business in comparison to 2,015 businesses answering this question in 2026.

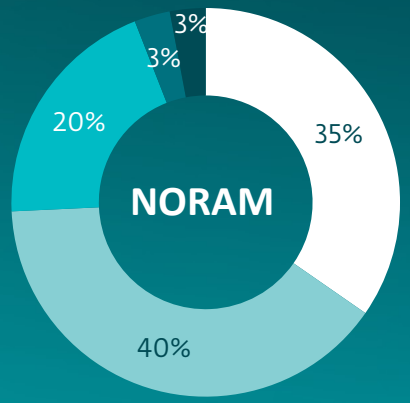
Average length of cyberattack investigation

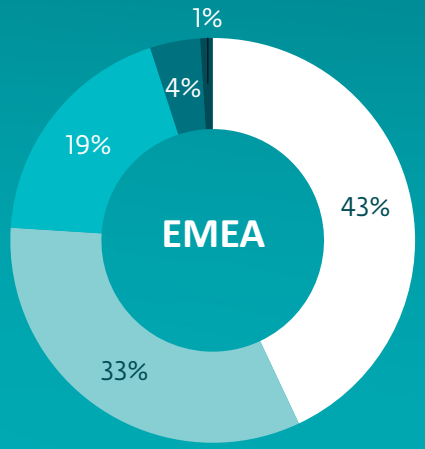


(values in %)

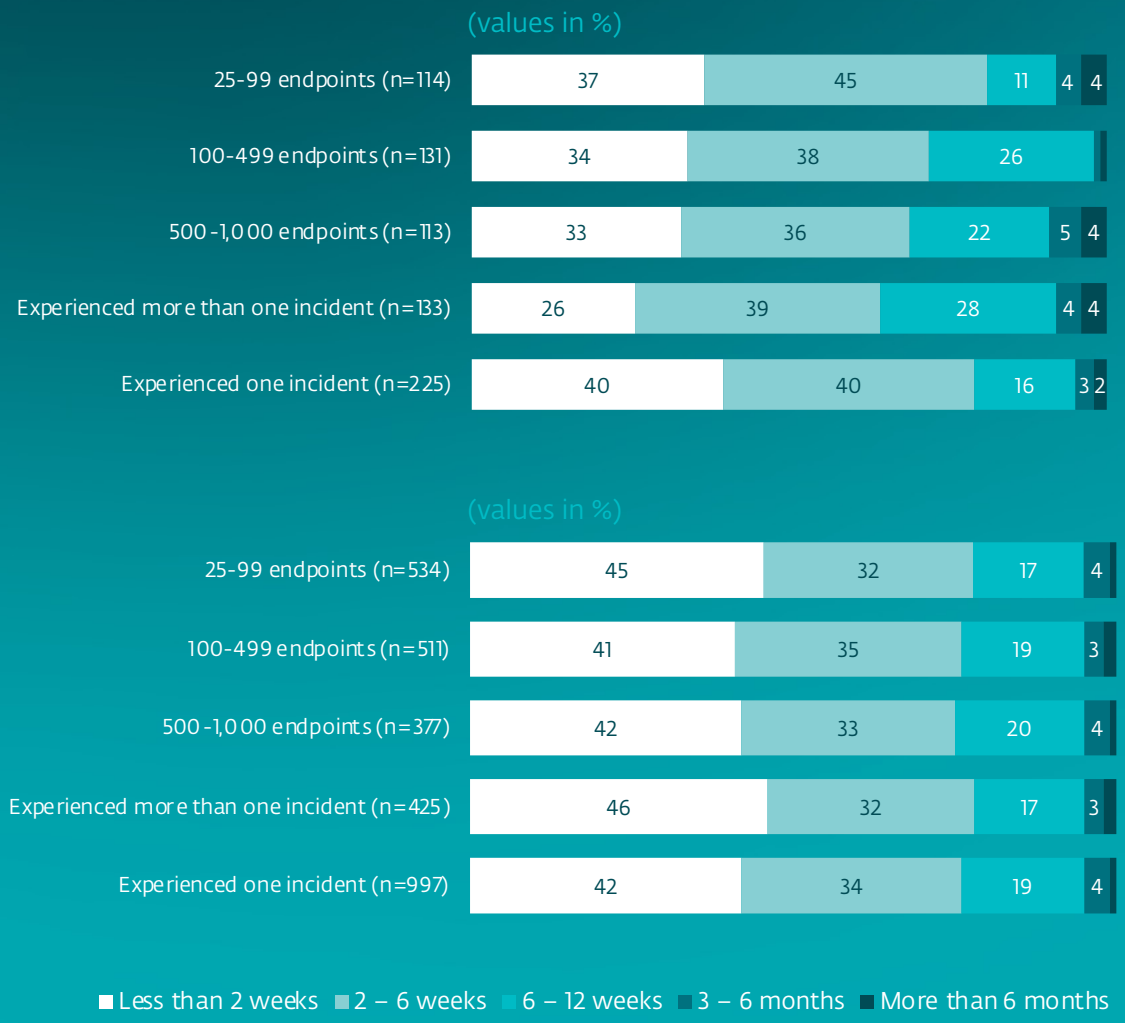


- Overall, a larger percentage of EMEA-based SMBs across all segments were able to perform incident investigation in less than two weeks compared to their North American counterparts.
- The number of North American SMBs completing incident investigations lasting two to six weeks exceeded their EMEA counterparts across all segments.



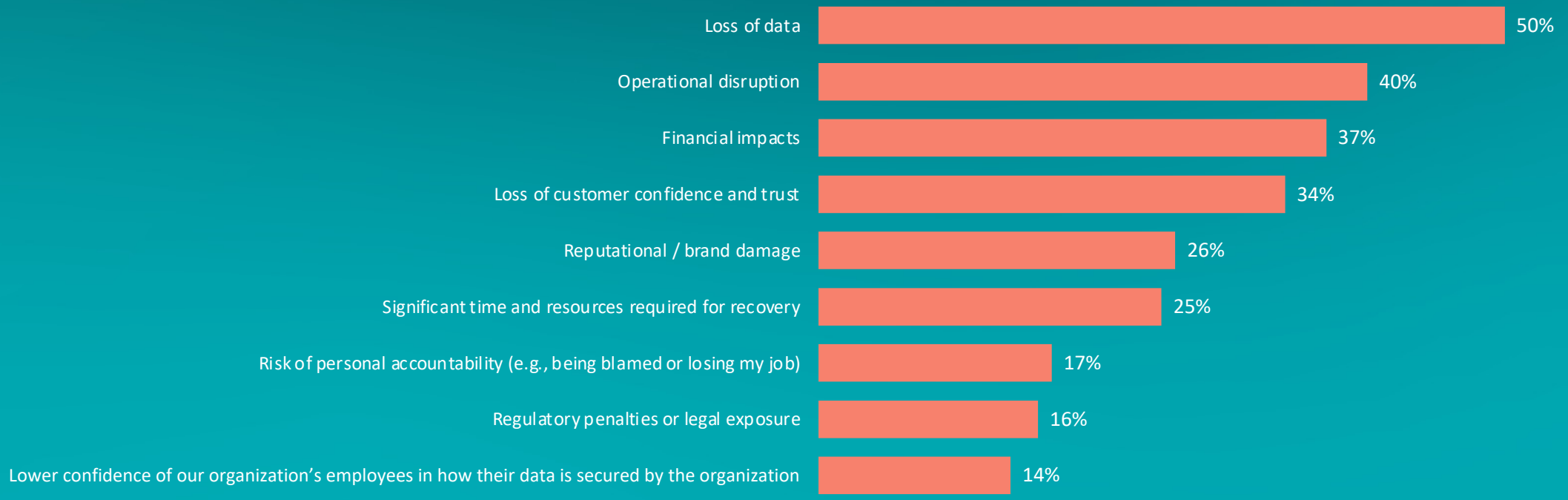


Average length of cyberattack investigation



Faster Incident Investigations Do Address The Most Feared Impacts Of The Cyberattacks Reported By Our Respondents

The biggest concerns in terms of business implications of cyberattacks



8

Conclusion

Moving Toward Resilience With Confidence

Michal Jankech

ESET, Vice President, Enterprise & SMB/MSP

While I wish I could say the door is closed on the phrase "we are too small to be attacked," it is clear that SMBs are taking cybersecurity more seriously.

The index shows a growing alignment between SMBs and security vendors, with more right-sized solutions and tailored services available. There is an increase in optimism and confidence, particularly in facing and surviving security incidents. Greater adoption of more capable security products, investments in services like Managed Detection and Response (MDR), or business continuity measures such as cyber insurance, all send a positive signal.

However, uncertainty remains. While 78% of SMBs recognize cybersecurity's strategic importance, inconsistent understanding of key threats, technology and terminology, including MDR and security posture, suggests there is still room for improvement. Any improvement will have to start with a reality check. We've found SMBs' concerns are often shaped by headlines on emerging threats like AI-driven attacks, while more routine risks—phishing, unpatched vulnerabilities and lack of monitoring — are underestimated. This hints that many respondents misperceive their security posture and resilience.

Still, the rising confidence reflected in the survey is a positive indicator of intent. But it's also a reminder of why a good relationship between provider and user is so important.

With no miraculous set-and-forget protection on the horizon for every threat out there, to truly reach the cyber-readiness and cyber-resilience milestones, SMBs must accurately assess their security posture, seek expert guidance and ensure continuous protection against threats that can disrupt their businesses.

9

About The Survey

About the survey

Topic
Cybersecurity in organizations across 13 countries

Target group
organizations with 25-1,000 endpoints
respondent is the main decision-maker around cybersecurity or influences decisions around cybersecurity.

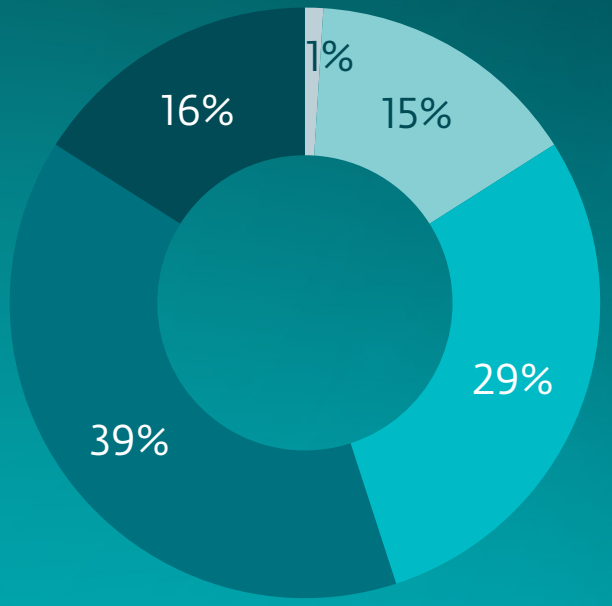
Total sample size
N=4,400

Survey Agency
Go4insight, member of ESOMAR (European Society for Opinion and Marketing Research).

The editors of the ESET SMB Cyber Readiness Index 2026 have elected to round figures to the nearest whole number across the report, creating a margin of error 1%.

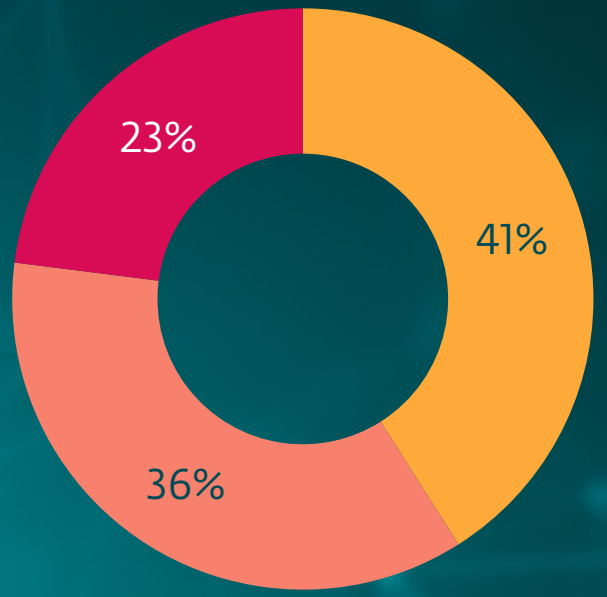
Country	Number of Respondents
Canada	200
Czech Republic	200
Denmark	150
France	500
Germany	500
Italy	500
Japan	500
Netherlands	100
Slovakia	200
Spain	400
Sweden	150
United Kingdom	500
United States	500
Total	**4,400**

Sample Structure



Number of employees

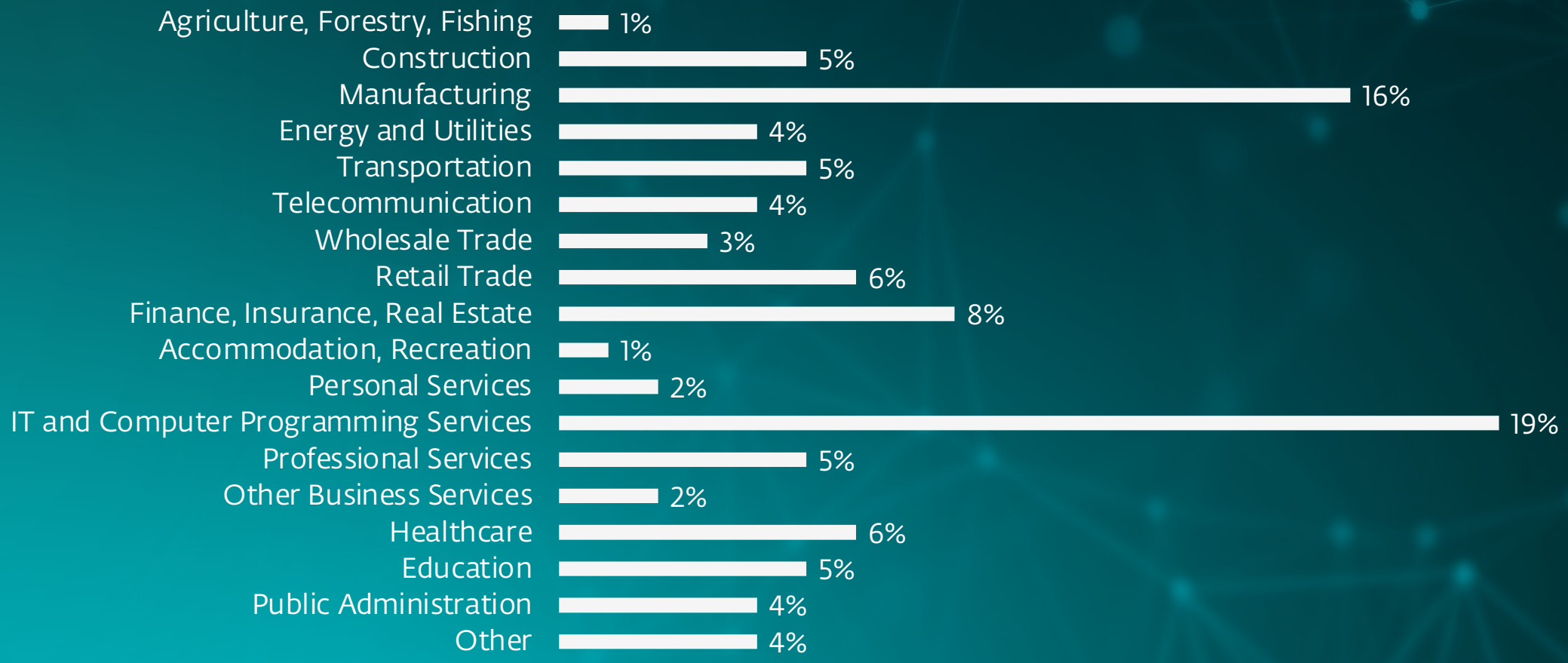
- Less than 25 employees
- 25-99 employees
- 100-499 employees
- 500-1,000 employees
- More than 1,000



Number of endpoints

- 25-99 endpoints
- 100-499 endpoints
- 500-1,000 endpoints

Primary industry



10

Appendix

This document is current as of 15 May 2026, and may be changed by ESET at any time.

Using data, statistics, figures and other information from the report is permitted if sourced properly: Cite the source as “ESET SMB Cyber Readiness Index 2026” and provide a link to the report. Citation must be in full and without modification. Any other use, including commercial use, is subject to prior written consent from ESET.

For additional information please contact ESET’s Public Relations Department at pr@eset.com.

Cybersecurity
Progress. Protected.

AI-Native Prevention For Tomorrow's Threats

Powered by 30+ years of human expertise,
11 Research and Development Centers around the globe
and local customer care.

www.eset.com