Press contact:
Florence Lievre
Tel.: +33 1 47 54 50 71
Email: florence.lievre@capgemini.com

69% of organizations believe that they will not be able to respond to cybersecurity threats without AI

Two in three organizations plan to deploy Artificial Intelligence to bolster their defense as soon as 2020

Paris, July 11, 2019 – Businesses are increasing the pace of investment in AI systems to defend against the next generation of cyberattacks, a new study from the Capgemini Research Institute has found. Two thirds (69%) of organizations acknowledge that they will not be able to respond to critical threats without AI. With the number of end-user devices, networks, and user interfaces growing as a result of advances in the cloud, IoT, 5G and conversational interface technologies, organizations face an urgent need to continually ramp up and improve their cybersecurity.

The "Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security" study surveyed 850 senior IT executives from IT information security, cybersecurity and IT operations across 10 countries and seven business sectors, and conducted in-depth interviews with industry experts, cybersecurity startups and academics.

Key findings include:

AI-enabled cybersecurity is now an imperative: Over half (56%) of executives say their cybersecurity analysts are overwhelmed by the vast array of data points they need to monitor to detect and prevent intrusion. In addition, the type of cyberattacks that require immediate intervention, or that cannot be remediated quickly enough by cyber analysts, have notably increased, including:

- cyberattacks affecting time-sensitive applications (42% saying they had gone up, by an average of 16%).
- automated, machine-speed attacks that mutate at a pace that cannot be neutralized through traditional response systems (43% reported an increase, by an average of 15%).

Facing these new threats, a clear majority of companies (69%) believe they will not be able to respond to cyberattacks without the use of AI, while 61% say they need AI to identify critical threats. One in five executives experienced a cybersecurity breach in 2018, 20% of which cost their organization over $50m.

Executives are accelerating AI investment in cybersecurity: A clear majority of executives accept that AI is fundamental to the future of cybersecurity:

- 64% said it lowers the cost of detecting breaches and responding to them – by an average of 12%.
- 74% said it enables a faster response time: reducing time taken to detect threats, remedy breaches and implement patches by 12%.
- 69% also said AI improves the accuracy of detecting breaches, and 60% said it increases the efficiency of cybersecurity analysts, reducing the time they spend analyzing false positives and improving productivity.

Accordingly, almost half (48%) said that budgets for AI in cybersecurity will increase in FY2020 by nearly a third (29%). In terms of deployment, 73% are testing use cases for AI in cybersecurity. Only one in five organizations used AI pre-2019 but adoption is poised to skyrocket: almost two out of three (63%) organizations plan to deploy AI by 2020 to bolster their defenses.

"AI offers huge opportunities for cybersecurity," says Oliver Scherer, CISO of Europe's leading consumer electronics retailer, MediaMarktSaturn Retail Group. "*This is because you move from detection, manual reaction and remediation towards an automated remediation, which organizations would like to achieve in the next three or five years."*

However, there are significant barriers to implementing AI at scale: The number-one challenge for implementing AI for cybersecurity is a lack of understanding of how to scale use cases from proof of concept to full-scale deployment. 69% of those surveyed admitted that they struggled in this area.

Geert van der Linden, Cybersecurity Business Lead at Capgemini Group says *"Organizations are facing an unparalleled volume and complexity of cyber threats and have woken up to the importance of AI as the first line of defense. As cybersecurity analysts are overwhelmed, close to a quarter of them declaring they are not able to successfully investigate all identified incidents, it is critical for organizations to increase investment and focus on the business benefits that AI can bring in terms of bolstering their cybersecurity."*

Additionally, half of surveyed organizations cited integration challenges with their current infrastructure, data systems, and application landscapes. Although the majority of executives say they know what they want to achieve from AI in cybersecurity, only half (54%) have identified the data sets required to operationalize AI algorithms.

Anne-Laure Thieullent, AI and Analytics Group Offer Leader at Capgemini concludes *"Organizations must first look to address the underlying implementation challenges that are preventing AI from reaching its full potential for cybersecurity. This means creating a roadmap to address key barriers and focusing on use cases that can be scaled most easily and deliver the best return. Only by taking these steps can organizations equip themselves for the rapidly evolving threat of cyberattacks. By doing so, they will save themselves money, and reduce the likelihood of a devastating data breach."*

The report can be downloaded here.

Research Methodology

The research surveyed 850 senior executives, director level and above, spread across seven sectors: consumer products, retail, banking, insurance, automotive, utilities, and telecom. One fifth of the executives are CIOs and one in ten are CISOs in their respective organizations. Executives belong to companies headquartered in France, Germany, the UK, the US, Australia, the Netherlands, India, Italy, Spain, and Sweden. Capgemini also conducted interviews with industry leaders and academics, examining the current status and impact of AI in cybersecurity.

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, the United Kingdom and the United States. It was recently ranked #1 in the world for the quality of its research by independent analysts.
Visit us at https://www.capgemini.com/researchinstitute/

About Capgemini
A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.
Visit us at www.capgemini.com. *People matter, results count.*