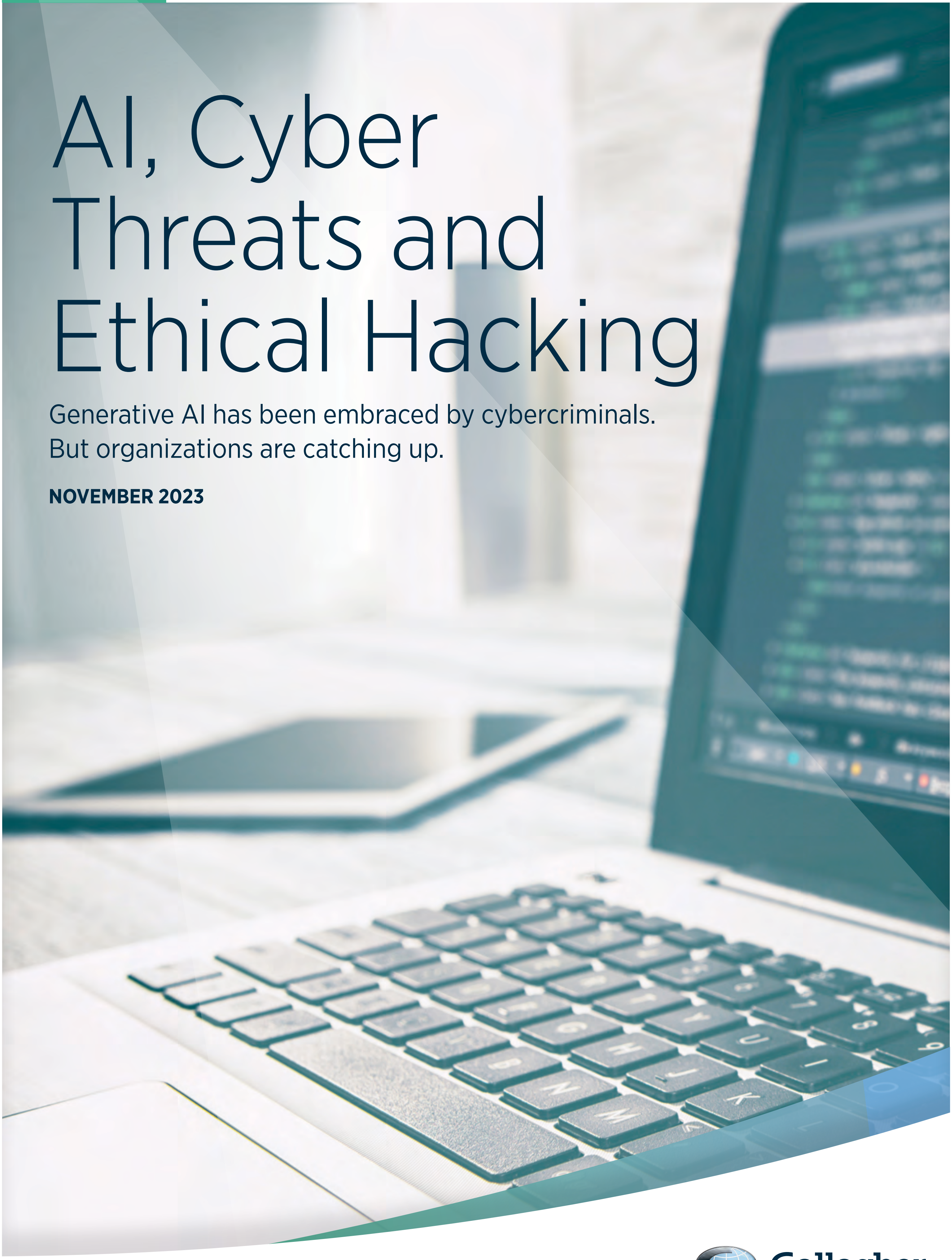
Spotlight SHIFTING PERSPECTIVES



AI, Cyber Threats and Ethical Hacking

Generative AI has been embraced by cybercriminals. But organizations are catching up.

NOVEMBER 2023

Insights

1 From more convincing phishing attacks to highly-engineered deep fakes, **cybercriminals are only just getting started when it comes to leveraging AI.** While the creators of generative AI tools never intended their deep-neural networks to be used for nefarious reasons, it is hard to close Pandora's Box once it has been opened. AI allows hackers to be more organized, targeted, and creative in their approach to common attack types.

2 The hackers may be one step ahead, but **cybersecurity is fast catching up.** Fifty-one percent of organizations have expanded the use of AI in their cybersecurity strategy over the last two years to tackle emerging challenges. AI tools can improve the sophistication of security practices and bridge the gap in qualified security resources.

3 As connected devices take over legacy technology, it becomes all the more challenging to continue detecting threats without the intervention of AI. AI's capability to learn faster and adapt makes it an **ideal technology to supercharge the role of the ethical hacker.** Automated vulnerability assessments and intrusion detection can reduce the time and effort needed for more routine tasks.

AI: Keeping pace with the cybercriminals

Generative AI has been embraced by cybercriminals. Operating outside of the checks and balances of the real world, they are already several steps ahead of cybersecurity teams. So how do businesses catch up?

From more convincing phishing attacks through to new methods of social engineering, including "deep fakes", malicious actors are using AI to increase the sophistication of their attacks and better target their activities. One example, shared by insurer Beazley,[1] is a classic example of CEO fraud, with a twist. The CFO of one of Beazley's insureds received a video message from someone who appeared to be the organization's CEO. The video failed and a conversation continued via chat.

The CFO was informed the company was going through a major business transaction which required funding and was told a lawyer would be in touch with the details. Completely convinced, the CFO authorized the transfer of multiple funds totaling over $6 million to the scammers over a two-week period.

The incident highlights the growing sophistication of social engineering, with AI being used to manipulate faces, voices, and other biometric markers in images, audio, and video.

The sophisticated technology makes it all the more difficult to determine what is real from what is fake, particularly to the untrained eye.

Research suggests AI is increasingly being used to create convincing deep fake attacks.[2] "If you're an attacker, why wouldn't you try and clone someone's voice and say, 'It's me. I'm at a boat show. Can you send five grand over?'" asks Johnty Mongan, Global Head of Cyber Risk Management at Gallagher. "They only have to get it right once and they can try it out with dozens of different companies."

"The [hackers] can spend all day doing it and are constantly learning. Whereas a company which is the victim of a deep fake attack has had no time to practice. Our clients don't have the same bandwidth when it comes to countering these increasingly convincing threats."

Next-generation cyber attacks

Cybercriminals are only just getting started when it comes to leveraging AI. While the creators of generative AI tools never intended their deep-neural networks to be used for nefarious reasons, it is hard to close Pandora's Box once it has been opened.

"I used to do a demonstration of how ChatGPT could write me a bash script to go and hack an organization," says Mongan. "But it got very good at picking up on the fact that this is a bad thing to do. But you can still ask it to give you an example of how you would write that malicious script. As long as an attacker uses the right terminology when using LLMs [large language models], they can almost get their own exploits written and checked for them."

Research suggests that AI-generated phishing emails are more likely to be opened than those which are manually created.[3]

"One of the telltale signs of a phishing email used to be that it was poorly worded and contain spelling mistakes, etc.," explains Mongan. "Whereas ChatGPT can write amazing emails convincing finance directors to approve a £10,000 payment, for instance. So if the email is 20% better, then it is 20% more likely to be clicked and, at that scale, it becomes very profitable for a criminal."

Seventy-five percent of security professionals say they have seen an uptick in attacks over the past year, with 85% attributing the rise to bad actors using generative AI, according to research by Sapio and Deep Instinct.[4] Nearly half of those surveyed said they believe generative AI will leave businesses more vulnerable to cyber attacks in the future.

AI-enabled offensive tools can automate malware, execute highly-targeted attacks, and intrude into the most carefully orchestrated security programs. These technologies help hackers to be more organized, targeted, and creative in their approach to common attack types.

Many companies are unwittingly expanding their attack surface in an effort to build a hyperconnected digital environment. As businesses embrace rapid digitization and expand their reliance on IT infrastructure and supply chain networks, they expose their data and intangible assets to an evolving, more complex risk landscape.

The expansion of digital footprints, alongside a growing shortage of talent within cybersecurity and a shift towards hybrid working is making it more and more difficult for organizations to protect their digital systems and assets. Organizations have arguably never been more vulnerable.

Keeping up with the hackers

The need to build a robust defense is therefore critically important. The hackers may be one step ahead in how they are leveraging AI to extort more money from businesses, steal more sensitive data and IP, but cybersecurity is fast catching up. Fifty-one percent of organizations have expanded the use of AI[5] in their cybersecurity strategy over the last two years to tackle emerging challenges.

In cybersecurity, AI has a diverse range of use cases in quantifying risk and detecting network attacks, traffic anomalies, malicious applications, and system vulnerabilities. AI tools can make security practices more advanced, offering teams the technology to handle a growing onslaught of breaches and bridge the gap in qualified security resources.

"If you can't beat them, you can join them," says Mongan. "We use a surface monitoring tools called SpiderFoot,[6] which searches for potential vulnerabilities surrounding an organization. By using AI to speed up processes you can detect whether you had dozens of attacks from a particular IP address during a particular period, for instance, and get a machine to block that IP address."

"Darktrace[7] is a prevalent EDR [endpoint detection and response] tool which places a sensor on your network and learns what is normal," he continues. "It looks for anomalies rather than signature-based threats and it can crunch data much better than a human being."

White hats on the counteroffensive

AI's capability to learn faster and adapt makes it an ideal technology to supercharge the role of the ethical hacker. Over the past decade, ethical hackers — or "white hats" — have become an important asset of cybersecurity teams. Their role in simulating real-world attacks and rooting out vulnerabilities in a firm's security posture has become an essential tool to improve overall cyber resilience.

Automated vulnerability assessments and intrusion detection can reduce the time and effort needed for more routine tasks. As connected devices take over legacy technology, it becomes all the more challenging to continue detecting threats across tech stack and systems (where multiple technology solutions are layered together) without the intervention of AI.

There is no doubt that AI tools offer to make ethical hackers' jobs more convenient by introducing smart automation to repetitive tasks, dramatically speeding up the ability to process information,[8] while spotting patterns that may not be apparent to the naked eye. A growing number of cybersecurity experts are leveraging AI tools to make short work of what were previously cumbersome processes.

Over half of white hats recently surveyed (55%)[9] say generative AI has increased the value of ethical hacking and security research, according to research by Bugcrowd. And one-in-five (21%) say that tools such as ChatGPT are already outperforming them. A significant proportion (78%) think it will disrupt how they carry out activities such as penetration testing and bug bounty programs in the next five years.

"It's not unreasonable to think of cybersecurity being done completely by AI," says Mongan. "All of these attacks are ultimately just IP addresses talking to IP addresses. So if we get good enough with AI, we could use it for anomaly detection and signature-based threats and then tell it what to do when an issue arises."

Some of the ways in which cybercriminals are currently leveraging AI[11]:

- Creating deepfake data
- Building better malware
- Stealth attacks
- AI-supported password-guessing and CAPTCHA-cracking
- Generative Adversarial Networks (GANs)
- Human impersonation on social networking platforms
- Weaponizing AI frameworks for hacking vulnerable hosts
- Deep exploits
- Machine Learning (ML)-enabled penetration testing tools

The global artificial intelligence (AI) in cybersecurity market size is expected to hit around **$102.78 billion by 2032.**[12]

51% of organizations have expanded the use of AI into their cybersecurity strategy over the last two years.[5]

Will AI replace the white hat role?

We are living in a time when many of us, both within and outside the tech space, are questioning whether our jobs are under threat from AI. Seventy-two percent of security experts polled by Bugcrowd do not think generative AI can completely replace human creativity in security research and vulnerability management. But clearly the role will evolve.

Mongan envisages a future where white hats could turn their hand to building the AI security programs that carry out tasks such as penetration testing and staying up-to-date with the latest threats in order to put together a robust offensive. "That would help us stay in line with the attackers," he says.

In the short to medium term, AI adoption should at least help to overcome the skills shortage within cybersecurity. According to the US Bureau of Labor Statistics, information security analyst roles will grow by 35% between 2021 and 2031.[10] The challenge even then is the sell-by-date on knowledge, according to Mongan. And in the rush to outsource and put everything in the cloud, some of the basics are being forgotten.

"Everything I learnt at university is irrelevant," he says. "I did one of the first computer science degrees where I would carry around textbooks on html coding and bash scripting, you passed an exam on your ability to code and everything was manual. Fast forward now to a language-based program like ChatGPT and it's fluent in all the coding languages and can write the bash script for you."

"After six or 12 months in technology you need to be onto the next thing. In just my short tenure so much has changed. It's just like Moore's law, where every year the adoption of technology doubles. IT managers are becoming contract managers — they don't have any of their own infrastructure — and we're losing the basic skills of, 'How do you build a PC?' and, 'How do you plug a LAN cable?'"

What is an ethical hacker?

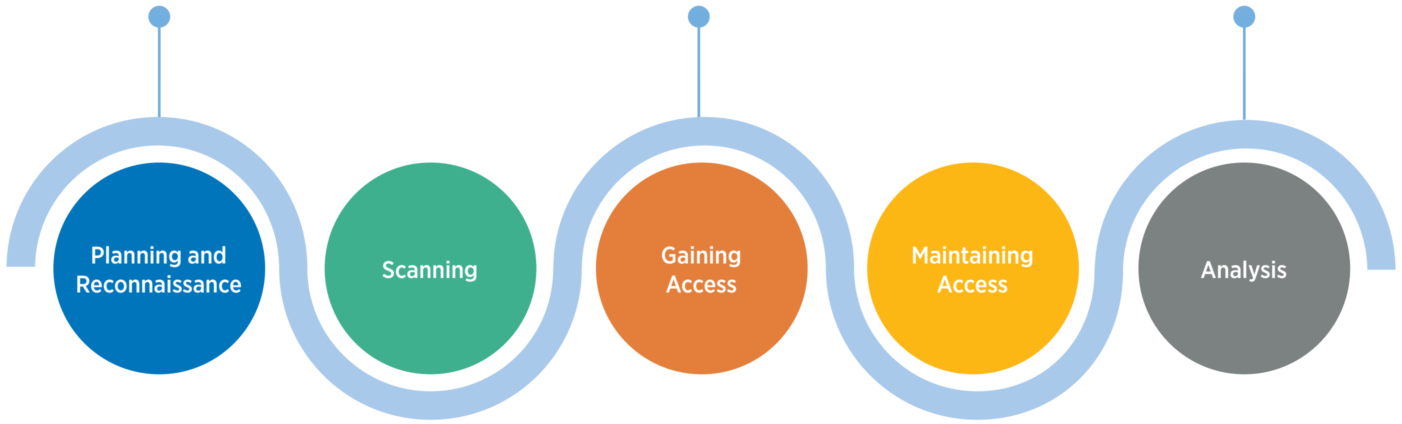
An ethical hacker, or white hat, is an individual who uses hacking skills to identify security vulnerabilities in an organization's infrastructure. Unlike malicious hackers, they seek vulnerabilities in an organization's system with prior consent.

Penetration Testing Phases

- Test goals are defined
- Testers covertly discover and collect information about the system

- Testers exploit vulnerabilities and mimic a real attack to breach the system

- Testers compile all the results for an in-depth report to understand system vulnerabilities and scope of security improvements

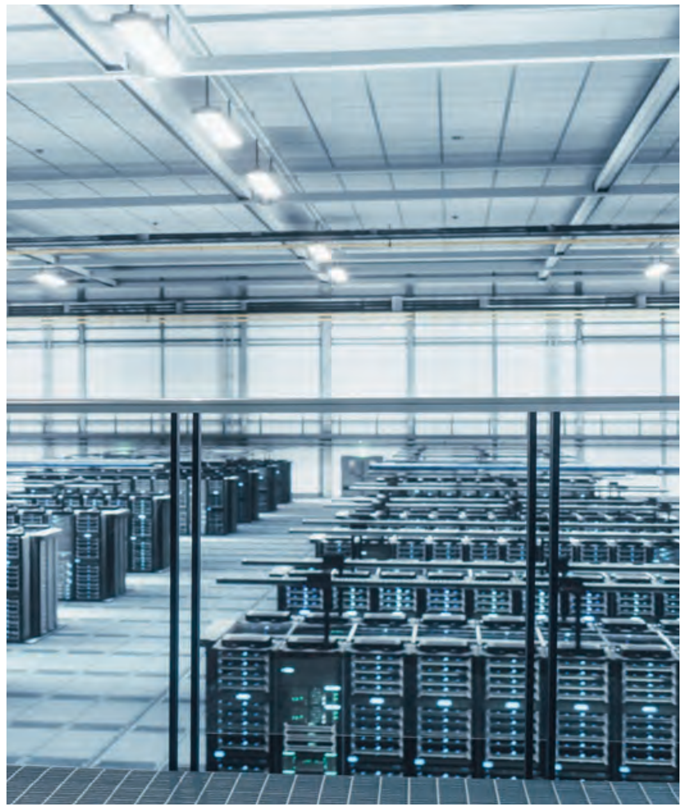


Conclusion

Major strides in digitization, including the emergence of generative AI, have dramatically expanded organization's digital capabilities. But with the vast opportunities on offer from this new generation of technologies, there are also new threats and exposures.

These technologies are not just being adopted by the corporate world. They are already in the hands of cybercriminals, actors who are not constrained by the rules, checks, and balances of a commercial enterprise.

Moving forward, it is essential for organizations to keep pace with the changing threat environment, and to make the right investments to counter the risk of attack, and to protect people and systems. The ethical hacker, armed with an evolving armory of generative AI tools, will be better positioned to fight back and iteratively improve an organization's cyber resilience posture.



Citations

1 https://www.beazley.com/en-us/articles/six-million-dollar-scam-reveals-extent-deepfake-ai-threat

2 Ironscales, "How will Cyber Attackers use AI? | ChatGPT & Phishing," 8 December 2022.

3 Violino Bob, "Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most," CNBC, 13 September 2022.

4 https://www.deepinstinct.com/voice-of-secops-reports

5 "The state of cybersecurity and third-party remote access risk", Ponemon Institute.

6 https://www.spiderfoot.net/attack-surface-monitoring/

7 Darktrace, "A CISO's Guide to Cyber AI"2023.

8 "Artificial Intelligence vs. Human Intelligence", Simplilearn, 5 June 2023.

9 "2023 Inside the Mind of a Hacker Report," Bugcrowd.

10 "Information Security Analysts", U.S Bureau of Labor Statistics.

11 Meah John, "AI in Cybersecurity: The Future of Hacking is Here", Techopedia, 6 July 2023.

12 "Artificial Intelligence (AI) In Cybersecurity Market", Precedence Research.

Spotlight

Gallagher

Welcome to Spotlight — presenting insights, shifting perspectives, and reframing evolving global trends.

Presenting the issues, opportunities, and risks that are transforming the way we do business, from industry hot topics and emerging growth markets through to perspectives on the big questions shaping our world today, this article provides actionable insights and analysis to inform strategic decision-making and power onward growth plans.

The Spotlight content series is designed for company executives, risk managers, industry operators, and business owners looking to reframe pressing issues, shape strategy, and pursue their future ambitions with confidence.

AJG.com/Insights

AJG.com **The Gallagher Way.** Since 1927.

The global news agenda and industry reporting is rapidly evolving at this time. Insights, concepts and perspectives presented in this report are relevant at time of publishing and may be subject to ongoing change as events and prevailing risks continue to evolve.

CONDITIONS AND LIMITATIONS
This information is not intended to constitute any form of opinion nor specific guidance nor legal or financial advice, and recipients should not infer such from it or its content. Recipients should not rely exclusively on the information contained in the bulletin and should make decisions based on a full consideration of all available information. We make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. Our advice to our clients is provided subject to specific terms and conditions, the terms of which take precedence over any representations in this document. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient's reliance upon any information we provide and exclude liability for the statistical content to fullest extent permitted by law.