Cyber risk

A specialist approach

Protecting your world | Miller

Growing cyber exposures deserve expert insurance

An organisation's capacity to manage and contain cyber risk has become a commercial imperative. The benefits of technology are clear, but a reliance on technology has increased organisations' vulnerability to cyber risk. Whether it's a major outage or a data breach, the potential financial and reputational losses from a cyber event can be devastating.

Given the growing relevance of cyber risk, and the limited protection afforded by traditional insurance products, the take-up of cyber insurance is growing rapidly. The cyber insurance market is now highly competitive with a diverse range of insurers offering broad cover and meaningful limits that can be tailored to meet the needs of companies of all sizes and sectors.

Miller has been placing cyber insurance in the London market for over a decade. Our market insights and expertise enables our team to construct cyber insurance that is tailored to each organisation's needs and that compliments existing insurance.

67%

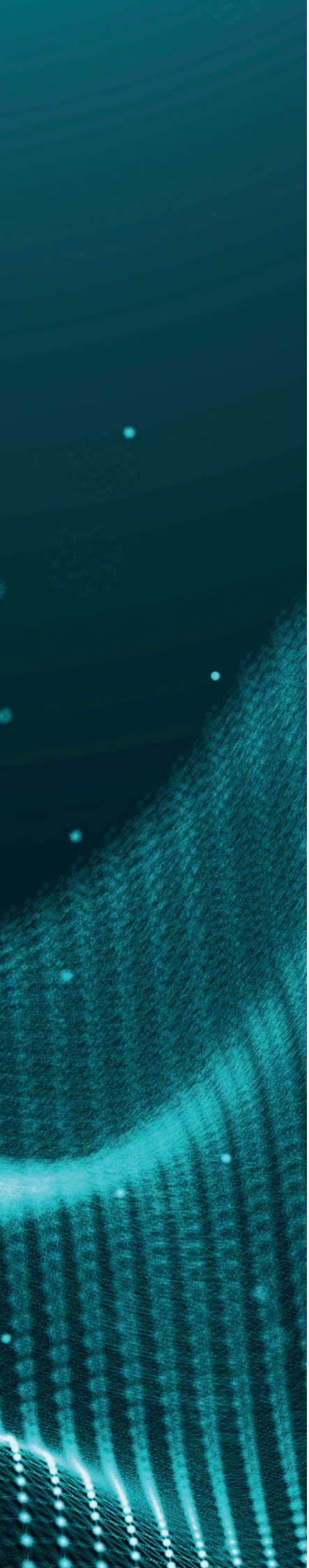
increase in security breaches in the past five years *

USD10.5tn

the cost of cyber crime per year by 2025 **

* Ponemon The Cost of Cybercrime 2020 Report

** Source: Cybercrime Magazine Report 2020



Contents

Business impact	1
Cover in action	3
Shaped by client needs	5
Expert advisor for complex risk	6
Smart analytics	7
Our team	8
About Miller	8

Business impact

Cyber incidents, whether the result of malicious intent or human error, can have a material impact on an organisation's finances and reputation. The immediate costs of responding to a cyber attack or major outage can run to the many millions of dollars, but will be significantly higher where there are business interruption, legal and regulatory consequences.

Data breaches can trigger regulatory actions and litigation

Cyber losses are particularly damaging for incidents that involve the loss of personally identifiable data, especially in territories with mandatory notification requirements such as the US and EU. In addition to the expense of managing a breach, organisations can face costly regulatory investigations and large penalties – fines under the GDPR can be as high as EUR20 million, or 4% annual global turnover. Increasingly, data breaches also give rise to litigation as investors, commercial partners and consumers seek compensation or to recoup their losses.

Business downtime costs are a key concern

Business interruption following a cyber event can give rise to large losses from lower revenues and lost business opportunities, as well as the cost of restoring systems and workarounds. Business interruption is the main cost driver behind cyber claims. It accounts for around 60% of the value of all claims analyzed. ^

Reputational damage can have lasting effects

The way in which an organisation manages a cyber incident has a direct bearing on the ultimate cost, including potential damage to brand and reputation. A high profile data breach or a disrupted service can impact customer loyalty, as well as lead to regulatory actions and litigation long after the event.

^ Allianz Cyber Risk Trends Report 2020.

SolarWinds hack infiltrates US government networks

In December 2020 Network Tools Specialist SolarWinds disclosed that its Orion network had been breached. It was used as a means to penetrate US government networks, as well as many Fortune 500 companies. Affected organisations included: the US Treasury, Department of Homeland Security, Department of Justice, NATO, the UK government, European Parliament and a host of Fortune 500 companies including Microsoft. The attack goes to show that even the world's best protected organisations are still vulnerable to cyber-attacks.

^ IBM Cost of a Data Breach Report 2020. ^^ Herjavec Group 2019 Cybercrime Report.

Cover in action

A disgruntled employee leaks personal data

Business impact

An employee undergoing disciplinary action publishes the personal data of millions of customers online. The company is required to notify the regulator and contact potential victims. Subsequently the regulator fines the company and investors and consumers launch civil litigation.

How Miller cover can respond

IT forensic services help identify the source of the leak, while crisis management services limit the reputational damage. The cyber policy picks up the defence costs of subsequent litigation and regulatory investigation.

Cyber criminals target company with ransomware

Business impact

An employee opens a phishing email and introduces ransomware to a company's network, encrypting critical customer data files. The company decides to close down its network as it reinstates systems.

How Miller cover can respond

Breach response services take immediate effect and are able to identify the source of attack and get the business back up and running within days, limiting downtime. The policy covers the first party costs, as well as potential business interruption and additional costs of workarounds.

An operational error leads to a network failure

Business impact

A hardware failure at a global airline causes an unplanned outage of critical systems. Although the systems were quickly restored, a mistake by an IT contractor damages the IT infrastructure. The resulting business interruption lasts over a week, costing tens of millions of dollars in lost business and compensation paid to passengers.

How Miller cover can respond

A bespoke cyber insurance policy covers the first party cost of rebuilding IT systems and lost data. The policy provides crisis management services to minimise the reputational damage, as well as indemnify the cost of passenger compensation, workarounds and loss of profits.

Google fined GBP44m for breaching GDPR rules by French regulator

In 2018 Google was hit with a record GBP44m (EUR50m) fine by French data regulator CNIL. The fine was levied for a 'lack of transparency, inadequate information and lack of valid consent regarding ad personalistaion.' The group claimed google did not have a valid legal basis to process user data for ad personalization.

A suspected terrorist group hacks into an industrial control system

Business impact

An unwitting employee introduces malware into a utility company's network through a compromised USB stick. Hackers use the malware to gain access to industrial control systems, resulting in a fire and explosion that causes property damage and forces the closure of the plant.

How Miller cover can respond

A Miller policy can provide coverage for physical damage resulting from a cyber event. This can be affirmative from the ground up, or via a "buy-back" of a cyber-exclusion on an insured's property or other package policies.

Scammers trick executive into transferring funds

Business impact

Fraudsters use information gleaned from social media and a spoof company email to impersonate a supplier, tricking the finance director to wire funds to the criminal's account.

How Miller cover can respond

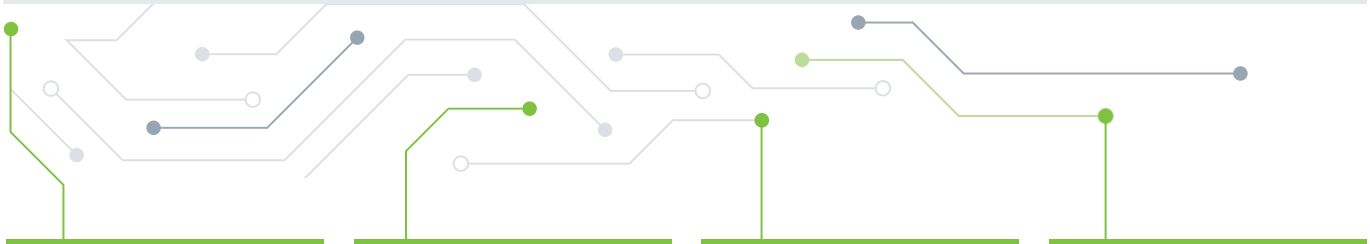
Policies can indemnify insureds for their monetary loss when employees were misled into transferring money, securities or ssets to an unintended third party.

Shaped by client needs

Large losses and increased regulation have raised awareness of cyber risk at a board level and have driven growing demand for specialist cyber insurance.

The current US standalone cyber insurance market is estimated at USD2.5 - USD3.5 billion annually.*

Organisations are buying cyber insurance for a host of reasons.



To address regulatory and legal concerns

Data protection regulations are getting tougher and litigation is increasing, creating ever larger privacy exposures. Cyber insurance can protect against third party liability and regulatory costs while breach response services can help meet breach notification requirements.

For speed of response

The ability to respond quickly and effectively has a direct impact on the cost of a cyber incident. Cyber insurance can give instant access to critical breach response services that have been proven to mitigate business interruption losses and the impact of a privacy data breach.

To comply with commercial requirements

Increasingly companies need to demonstrate cyber insurance cover when tendering for contracts. Organisations also buy cyber insurance to protect against cyber risks in the supply chain, including business interruption and third party liabilities.

For coverage and contract certainty

Cyber insurance can provide contract certainty by addressing gaps or exclusions in traditional cover and offering appropriate limits. Standalone cyber insurance also provides protection for losses that are not covered by traditional property and casualty insurance, such as systems outages.

* Source: 2018 PwC Report 'Findings from PwC's global cyber insurance survey.'

Expert advisor for complex risk

Insurance can form a key part of an organisation's response to managing cyber risk, but evaluating, mitigating and transferring cyber risk is not a tick box exercise. It requires a trusted and expert advisor to guide the buyer through the process.

It's not only important to offer the right cover, cyber insurance also needs to align with existing coverages.

Client needs first

When arranging cyber insurance we start with the needs of the client. Each organisation has its own specific exposures and concerns, risk appetite and response capabilities. For some companies the focus will be on breach response services and third party liabilities, for others the focus will be protecting the balance sheet against supply chain disruption or a major outage.

Miller offers a wide range of solutions and services, made to fit client requirements - from off-the-shelf cyber policies for SMEs to complex bespoke solutions for large corporates.

Access to leading cyber market

There are around 75 insurers offering cyber insurance in the Lloyd's market, home to the world's centre of excellence for cyber risk and insurance, as well as supporting services such as legal and claims. Our access to Lloyd's enables us to deliver bespoke solutions, arranging coverage and high levels of capacity that cannot easily be placed elsewhere.

our team's cyber experience dates back to 1997

Our team

Debbie Hobbs | Head of Cyber
T +44 20 7031 2735
M +44 7711 041 191
debbie.hobbs@miller-insurance.com

Simon Milner | Account Executive
T +44 20 7031 2506
M +44 7973 297 544
simon.milner@miller-insurance.com

Danny Cooper | Account Executive
T +44 20 7031 2964
M +44 7833 298 396
danny.cooper@miller-insurance.com

Umber O'Doherty | Cyber Counsel
T +44 20 7031 2540
umber.o'doherty@miller-insurance.com

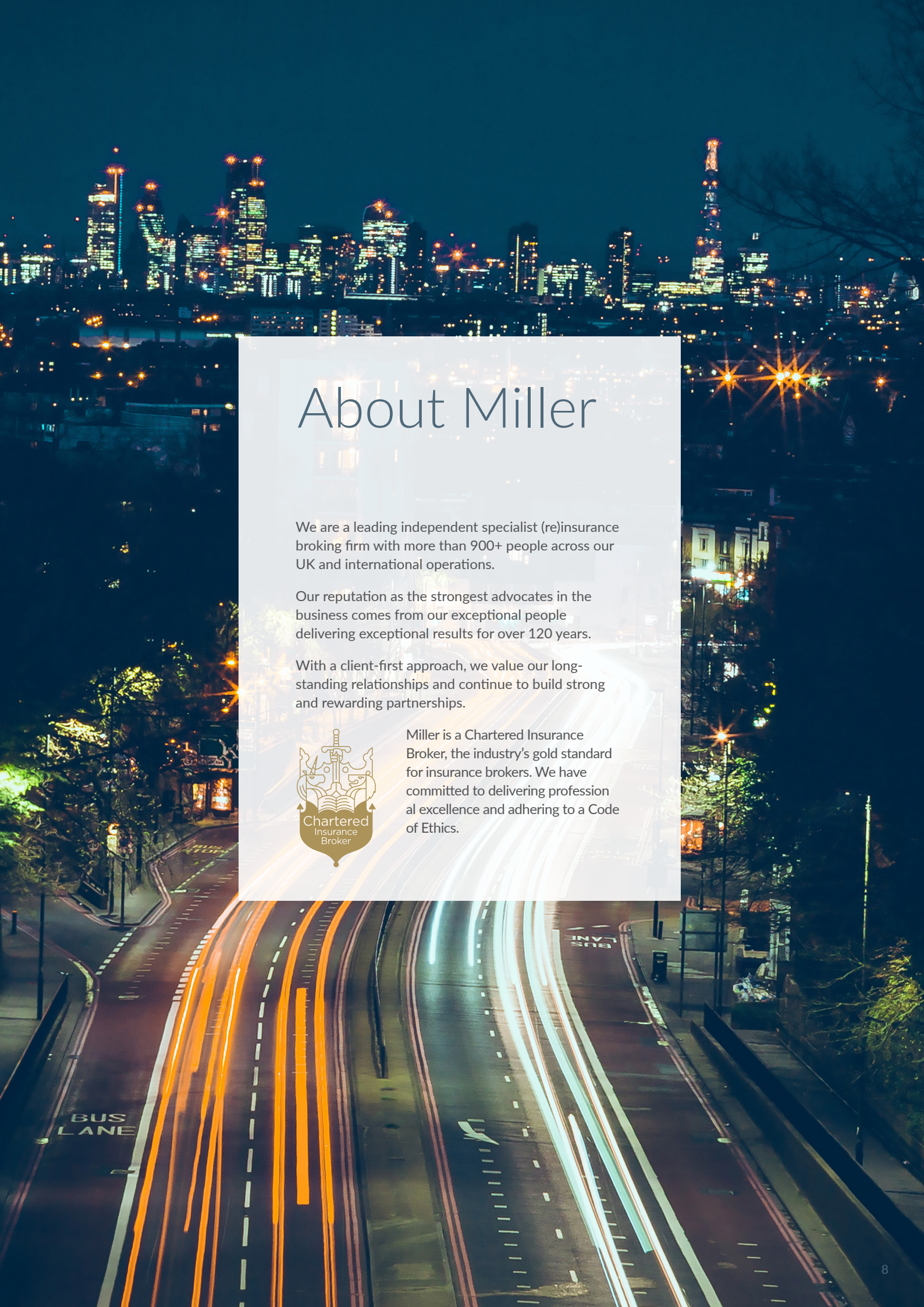
Samuel Jobling | Account Executive
T +44 20 7031 2499
M +44 7726 345 540
samuel.jobling@miller-insurance.com

Darcy Hapkewcz | Account Handler/Broker
T +44 20 7031 2551
darcy.hapkewcz@miller-insurance.com

Luke Pordham | Account Handler/Broker
T +44 20 7031 2728
luke.pordham@miller-insurance.com

Tom Cahill | Account Handler
T +44 20 7031 2667
tom.cahill@miller-insurance.com

"Our access to Lloyd's enables us to deliver bespoke solutions, arranging coverage and high levels of capacity that cannot easily be placed elsewhere."



About Miller

We are a leading independent specialist (re)insurance broking firm with more than 900+ people across our UK and international operations.

Our reputation as the strongest advocates in the business comes from our exceptional people delivering exceptional results for over 120 years.

With a client-first approach, we value our long-standing relationships and continue to build strong and rewarding partnerships.

Chartered Insurance Broker

Miller is a Chartered Insurance Broker, the industry's gold standard for insurance brokers. We have committed to delivering profession al excellence and adhering to a Code of Ethics.

Miller
70 Mark Lane
London
EC3R 7NQ

T: +44 20 7488 2345
F: +44 20 7702 3555
miller-insurance.com

P352.03 0524 | © Miller 2024

Protecting your world | Miller