Cyber risk

A specialist approach

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.

* Source: Herjavec Group 2017 Cybercrime Report
** Lloyd's Facing the cyber risk challenge report 20 September 2016

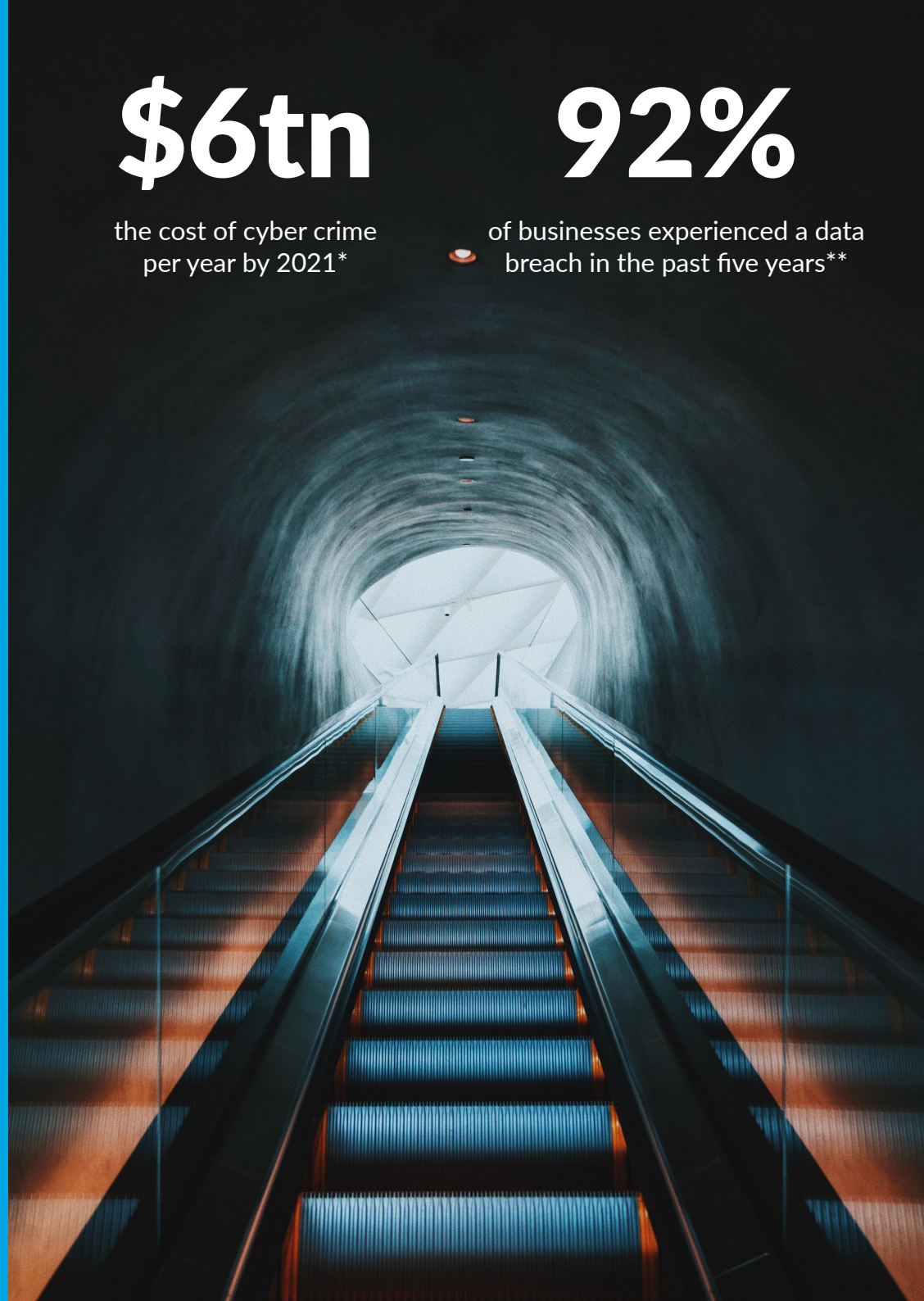
miller-insurance.com

$6tn

the cost of cyber crime per year by 2021*

92%

of businesses experienced a data breach in the past five years**



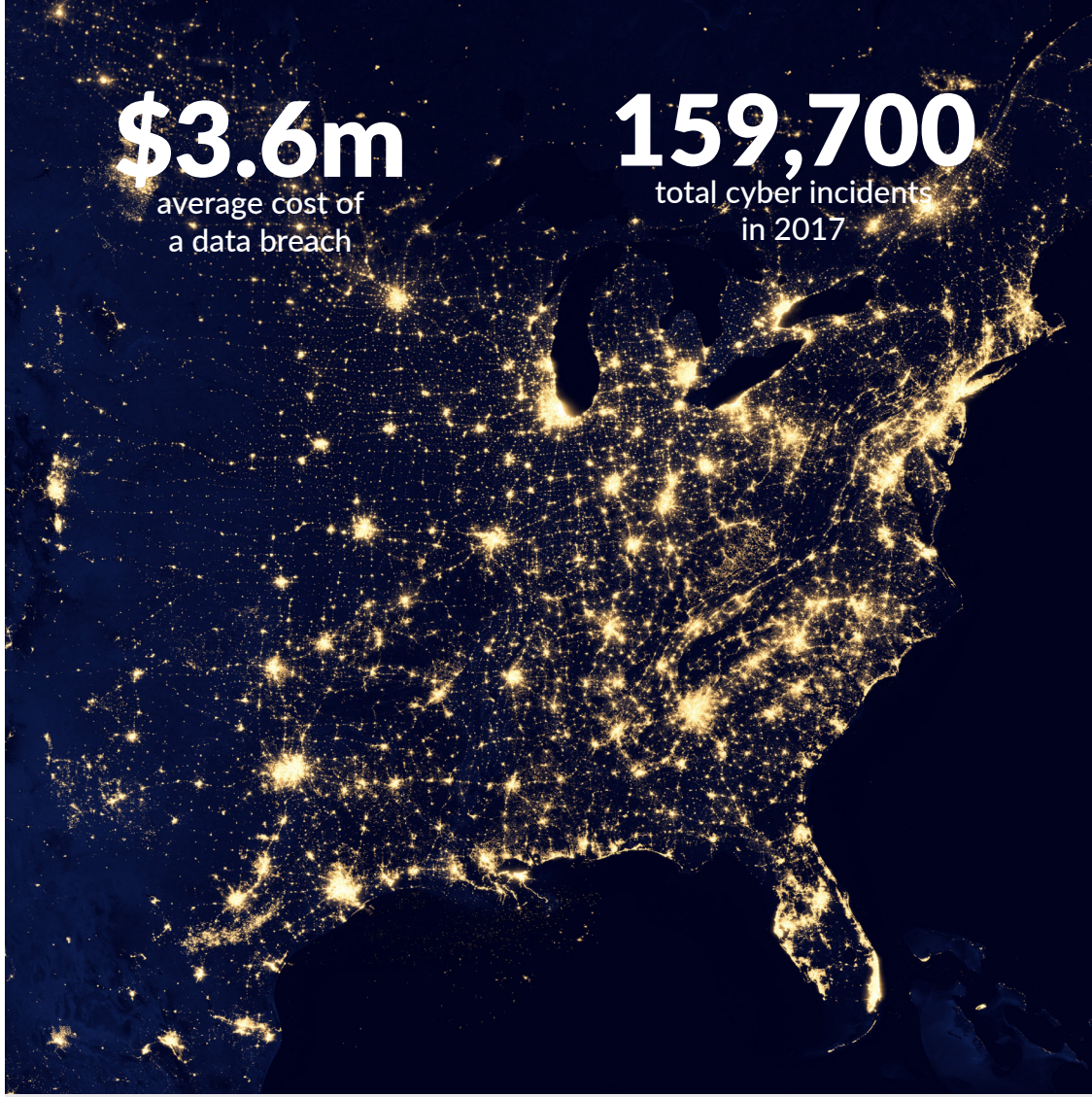
Business impact

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 €20 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. Estimates from Lloyd's of London suggest that an unplanned outage at a cloud service provider could cause business interruption losses as high as $15 billion for US businesses.
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.

^ 2017 Ponemon Cost of Data Breach Study

^ ^ The Internet Society 2017 Cyber Incident & Breach Trends Report



Airlines hit by systems outages

Recent years have seen a number of US and international airlines suffer financial loss and reputational damage from systems outages. In 2017, a mistake made by a contractor resulted in the shutdown of British Airways IT systems costing the airline $100m. A router failure at Southwest Airlines disrupted thousands of flights and cost an estimated $54m while an outage at Delta Air Lines resulted in $150 million in lost revenue.

Cover in action

	Business impact	How Miller cover can respond
A disgruntled employee leaks personal data	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.	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	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.	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	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.	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.
A suspected terrorist group hacks into an industrial control system	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.	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	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.	Policies can indemnify insureds for their monetary loss when employees were misled into transferring money, securities or assets to an unintended third party.

Cyber attack causes worldwide disruption

The WannaCry and NotPetya cyber attacks caused unprecedented disruption around the world in 2017, affecting hospitals, manufacturers, banks and professional services firms. Car manufacturers were forced to shut down production facilities while problems at container terminals cost shipping company Maersk an estimated $300m.

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. 83% of large US organisations now purchase standalone cyber insurance while penetration rates outside the US are rising.*

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 commerical 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: 2017 RIMS Cyber Survey

Critical infrastructure attack

In 2015 a cyber attack against Ukrainian power companies caused a blackout affecting some 250,000 people. The attack was the first known successful cyber attack against a power grid to cause major disruption, although there have since been other attacks against critical infrastructure. Hackers breached security defences at a flood control dam in the state of New York in 2016, while hackers compromised the safety system of an unnamed energy plant in the Middle East in 2017.

Expert advisor for complex risk

Cyber risk is evolving and increasing in complexity, and total elimination of the risk is clearly unrealistic. Despite increasing investment in cyber security, cyber protagonists appear to be one step ahead and even the most resilient of firms remain vulnerable to a cyber attack or old fashioned human error.

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.

Smart analytics

corax
Cyber Insurance Software

Through our partnership with risk modelling company Corax, we are able to offer cyber risk analytics that can more accurately quantify the potential for insurable loss and inform conversations around how much limit should be purchased.

Our approach is based on the most comprehensive view of cyber risk available anywhere in the industry. Leveraging data gathered from a variety of sources including financial reports, legal settlements, regulatory settlements, insurance claims and threat intelligence through dark web monitoring, this modelling framework indicates the potential economic loss from a variety of cyber events.

Our team

Our highly experienced cyber team has an in depth knowledge of the cyber insurance market and is able to leverage long-standing market relationships to obtain flexible cover on favourable terms.

Nick Fearon
T +44 20 7031 2498
M +44 7887 954 164
nick.fearon@miller-insurance.com

Tom Quy
T +44 20 7031 2694
M +44 7557 563 896
tom.quy@miller-insurance.com

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

Daniel Leahy
T +44 20 7031 2310
M +44 7980 388 547
daniel.leahy@miller-insurance.com

Holly Haylett
T +44 20 7031 2485
M +44 7940 453 709
holly.haylett@miller-insurance.com

Our team's cyber experience dates back to

1997

4,000+

polices placed by Miller

About Miller

Since Miller was founded in 1902, we have gone from strength to strength because of our unwavering focus on delivering an exceptional standard of service to our clients.

We are known for doing the right thing, delivering on our promises and working as one team.

Today, we are a leading specialist (re)insurance broking partnership, headquartered in London with more than 600 people across our UK and international operations.

Chartered Insurance Brokers

Miller is proud to hold Chartered Insurance Broker status, the industry gold standard awarded by the Chartered Insurance Institute (CII).

This title demonstrates our professionalism, client focussed approach and commitment to excellent service standards.

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

Tom Quy

Miller Insurance Services LLP

Miller Insurance Services LLP
70 Mark Lane
London
EC3R 7NQ
T +44 20 7488 2345

miller-insurance.com

Version P352.02 0618.MC |