
accenture
AXA
CITY OF LONDON
The Global Future of Cyber Insurance— and the London Market's Pivotal Role

Foreword

The City of London has a huge opportunity. One of the biggest threats facing large corporates and SMEs is cyber risk, and the London Market—with its world-leading cybersecurity expertise—offers insurers and cybersecurity specialists an unrivalled environment in which to provide unique and holistic end-to-end cyber resilience services.

This opportunity will allow London to bolster its position as a major, global cyber insurance market, supporting the success of those insurers that choose to underwrite in this innovative city.

Despite an increase in the frequency and severity of global cyber attacks, and recent privacy related regulatory changes such as GDPR; cyber risks worldwide remain profoundly under insured global cyber premiums in 2017 were less than 1%[1] of the estimated $600 billion[2] annual cost of cybercrime. While this presents insurers and brokers with an enormous potential market, the challenges involved in underwriting cyber insurance are significant. Historical incident data is scarce; cyber risks evolve at an extremely rapid pace and the potential for accumulation risk is both significant but extremely challenging to model.

Insurers that establish a strong grasp of these challenges have an opportunity to become market leaders in cyber insurance by developing new and unique propositions that focus not only on indemnification, but on truly understanding the specific cyber threats to clients, and helping protect against them. These offerings should include complete and transparent cyber risk assessments for clients; targeted, industry-specific risk mitigations; tailored cyber insurance products and coverages; and breach response services to effectively and efficiently restore clients to their pre-incident state. While no protection is foolproof, there are practical steps that can be taken to both reduce the overall cyber threat, as well as speed the recovery in the event of an incident.

To develop such propositions, insurers must leverage not just their existing core underwriting expertise, but also London's wider cybersecurity ecosystem. This will involve bringing together brokers, legal firms, cybersecurity vendors, analytics providers and threat intelligence specialists to provide the understanding and full set of solutions businesses require.

Against this background, London remains uniquely positioned for further successful growth as a centre for cyber insurance for the following reasons:

- Its longstanding global strength as an insurance market.
- The capital flexibility that the subscription nature of Lloyd's of London provides, which enables complex risks to be spread within the marketplace.
- The concentration and diversity of its cybersecurity talent pool.
- Its global mindset and the stable market regulatory environment.

These all play a role in fostering the innovation and collaboration needed to ensure that insurers can continue to serve their clients' evolving cyber resiliency needs.

Alderman Peter Estlin
The RT Hon
The Lord Mayor of London

Sushil Saluja
Senior Managing Director
Accenture Financial Services

Paul Greensmith
UK CEO of Legal Entities
AXA XL

James Tuplin
Head of Cyber & TMT
International Financial Lines, AXA XL

The frequency and severity of cyber incidents are increasing fast

As cyber threats continue to grow, companies' spending on defending themselves is rising in tandem.[3] And while these efforts are having some success, the frequency and severity of attacks continue to rise rapidly.[4]

Accenture's 2018 State of Cyber Resilience[5] found that organisations can now successfully ward off, on average, 82% of cyber-attacks, up from 70% in 2017. However, with the growing industrialisation of cyber-attacks and increasing sophistication of threat actors, the total number of attacks per company is also increasing—reaching an average of 232 per year in 2018, more than double the number reported the year before. It is estimated that cyber-attacks cost the global economy US$600 billion in 2017,[6] and that the total value at risk from cybercrime is US$5.2 trillion over the next five years.[7]

IMPACTS VARY BY INDUSTRY

The nature and effects of cyber risks vary by industry. For those sectors that handle a large amount of personally-identifiable information (PII)—such as financial services, healthcare and transportation—concerns tend to focus on the potential regulatory fines and reputational damage resulting from a data breach. Whereas those that hold less personal customer data—such as energy, marine, and the critical national infrastructure (CNI) sector, for example—worry more about the very material risk of business interruption from IT downtime.

The rapid, ongoing evolution in the cyber landscape is set to see these risks and costs continue to escalate. Companies must therefore continue to evolve their cyber resilience strategies in order to keep pace, and it is against this background that the opportunity for insurers and their partners presents itself.

The evolving world of the threat actor

The Tactics, Techniques, and Procedures (TTPs) that threat actors use to gain access to a company's infrastructure are myriad and ever-changing. Below we highlight some of the macro trends Accenture Security has observed over the last 12 months, and some of the potential evolutions to come.

MAKING A BUSINESS OF IT

Many threat actors have now evolved into highly organised cybercriminal groups, with sophisticated business models and stable revenue streams, and are engaged in a continual battle with law enforcement.

Traditional data breaches or targeted attacks often involve infiltration of a target company and the harvesting of critical data (such as credit card data) with an aim to monetize that data by selling it on the dark web or by using it to physically extract cash from ATMs or other devices. But, with law enforcement now having penetrated many parts of the criminal underworld, the traditional approach has become high risk, causing cybercriminals to switch tactics. It is now less risky, and more lucrative, to extort the data owner without moving any data anywhere by using ransomware or other malware to lock an organisation out of its data systems and disrupt critical business processes.

Ransom demands from threat actors to 'unlock' critical systems can run into the millions of dollars. Organised cybercriminal groups will target mid market firms they deem likely to pay the ransom and will use recent innovations such as 'wiper ware' (a type of destructive malware that erases data including logs used to monitor for suspicious activity) to make the attack harder to detect and repel and increase the pressure to pay the ransom. Accenture Security estimates the financial consequences of ransomware alone have increased 21 percent in the last year.[8]

A flourishing, entrepreneurial and globally connected ecosystem of illicit activity exists to support the organised cybercriminals. Small scale players post newly discovered technical software vulnerabilities to dark web forums with instructions on how to exploit this for a small fee. These vulnerabilities are picked up by larger more organised groups and industrialised into the next wave of ransomware and malware attacks.

NEW TECHNOLOGY, NEW OPPORTUNITY

New technologies, such as blockchain and artificial intelligence, create new opportunities for companies but they also present significant new opportunities for cyber adversaries, in a variety of innovative ways.

For several years, financially motivated hackers have made use of cryptocurrency as a key mechanism for laundering ill gotten funds and demanding ransom during extortive campaigns. Senior law enforcement officials estimated that, last year, cybercriminals crypto laundered US$4.2 billion to US$5.6 billion in Europe alone.[9] Accenture Security has observed adversaries across English and Russian speaking marketplaces offering cryptocurrency 'mixing' services, which enable users to hide their identities while exchanging bitcoins and alternative cryptocurrencies, such as Monero and Ethereum.

Another recently observed threat to blockchain and cryptocurrency is blockchain reorganisation, which was undertaken by malicious adversaries in early 2019. In what is dubbed a '51 percent attack,' adversaries stole nearly US$1.1 million in Ethereum Classic coins by hijacking more than 50 percent of the blockchain.[10] The adversaries were able to 'sell' Ethereum Classic coins for cash while rewriting the blockchain to steal both the cash and the coins.

One active area of cybersecurity research is around what security vulnerabilities the increasing adoption of AI may introduce. For instance, deep convolutional neural networks now routinely used for image recognition tasks can be fooled into misclassifying objects through specially constructed 'adversarial examples'.[11] The real-world consequences of this could potentially be severe, as it introduces fallibility into systems we increasingly will rely on in critical areas such as, for example, autonomous driving and the diagnosis of medical conditions.

PROTECTING AGAINST THESE EVER CHANGING THREATS REQUIRES A ROBUST DEFENSE—INSURERS AND THE WIDER ECOSYSYTEM WILL PLAY A CRITICAL ROLE

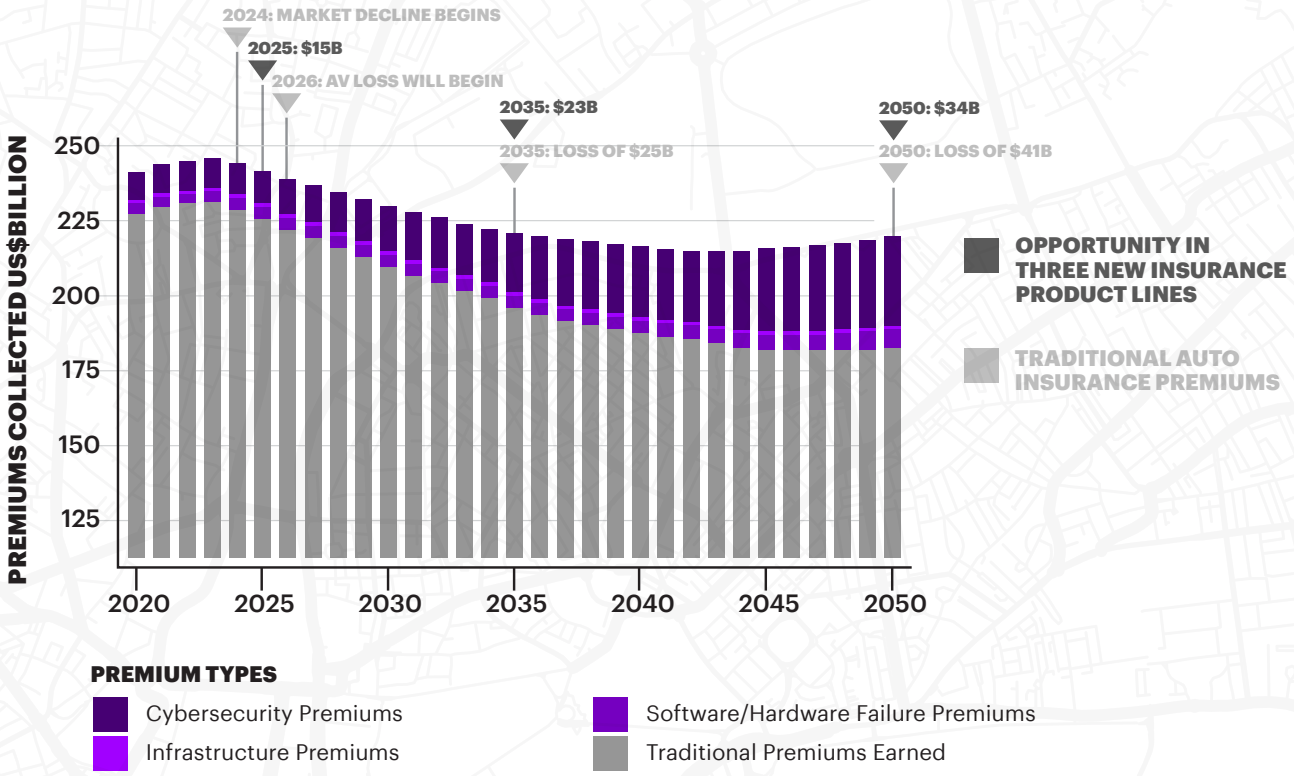
Clients' current underinsurance presents a major market opportunity

Despite estimated global premium growth of 30% compounded annually between 2011 and 2016, global cyber insurance premiums still totalled little more than US$3 billion in 2017, representing just 1% of total commercial insurance premiums.[12]

Major insurers worldwide are moving to meet this demand. Around 70 (re)insurance companies now offer standalone cyber policies across the globe, with data breach and business interruption being the main risks covered. In geographical terms, the US remains by far the world's largest cyber insurance market, accounting for at least 60%—and by some estimates, 90%—of global premiums.[13,14,15] Outside the US, however, the market is much less mature, and penetration of cyber insurance remains at less than 5%. Take-up of cyber insurance also varies by industry and client size, and with awareness of cyber risks increasing in sectors such as energy, aviation and marine, this significant level of under-insurance presents a huge opportunity for the London insurance market.

The current underinsurance of cyber risks—coupled with rising awareness and regulations such as the European Union's General Data Protection Regulation (GDPR) Directive—is likely to continue to drive increased demand in the market for cyber insurance. Technological advances such as autonomous vehicles will also fuel market growth. An Accenture study[16] of the autonomous vehicle market projects that the related cyber product liability and public infrastructure insurance premiums could total US$81 billion by 2025—with cyber insurance accounting for US$64 billion of this. (See Figure 1 for details of how this market represents a significant potential source of organic growth.)

Figure 1: Insurance opportunity map for autonomous vehicles, 2020-2050



Source: Insuring Autonomous Vehicles: An $81 Billion Opportunity by 2025, Accenture Research.

A LACK OF TRANSPARENCY MAKES CYBER EXPOSURES HARD TO QUANTIFY

While the opportunity for the insurance industry is clear, there are still significant risks and obstacles for insurers seeking to grow their cyber books of business. Two thirds of insurers surveyed by the OECD in 2017[17] identified concerns over 'the ability to quantify cyber exposure' as a key obstacle to writing new business. The lack of incentives for businesses to report cyber incidents means there is limited availability of historical data on losses. This is particularly the case for emerging cyber risks such as business interruption, as well as in less mature industries and markets. In addition to this, the regulators' position on new legislation such as GDPR is yet to be fully tested and may heavily impact the size of potential data-breach-type losses. Insurers will be particularly cautious around cyber aggregation risk, where a cyber-attack against a systemic point of failure—such as a cloud service provider—could simultaneously impact numerous insured clients.

Insurers also struggle to estimate the frequency of attacks due to the rapid evolution of threat actors. These now include nation states, organised criminal gangs and 'hactivists', all of whom are increasingly well-resourced and often possess a much greater focus on specific industries. These actors are often innovative and adept at leveraging new technologies. For example, 2018 saw a significant increase in cyber-attacks based on cryptocurrency miner malware.[18] New strategies are also emerging, such as targeting the weakest point in the supply chains of large corporates, which are typically less well defended than the company itself, but could provide an access point to its systems.

INSURERS NEED TO KEEP PACE WITH ADVANCES IN TECHNOLOGY

As well as understanding the complexities of cyber threats, underwriters also need to keep up to date on a vast amount of technical information. This includes known software vulnerabilities and security patches, the impact of emerging technologies such as the Internet of Things (IoT) and blockchain, and the different technology architectures, data and processes typically used in different industries.

This problem increases as demand for cyber coverage grows in industries that have not previously been particularly cyber aware. Clients also face challenges in understanding their own risks, meaning that the information provided from the end client via the broker can sometimes be incomplete. Together, these factors make it challenging to derive a clear technical price for cyber risks. Pricing therefore defaults to being strongly market-driven, lowering the barriers for market entrants with new capital driving down pricing.

The lack of incentives for businesses to report cyber incidents means there is limited availability of historical data on losses. This is particularly the case for emerging cyber risks such as business interruption, as well as in less mature industries and markets.

LIMITED RISK UNDERSTANDING UNDERMINES TRUST BETWEEN CUSTOMERS AND INSURERS

A recent survey[19] revealed that 75% of global underwriters and brokers of cyber insurance policies think that organisations "not understanding [their] exposure" is actually the biggest obstacle to their buying cyber insurance. This problem is particularly prevalent among small and medium-sized enterprises (SMEs), as they often lack the scale to maintain their own in-house cybersecurity teams. This may be for one or more of the following reasons:

1. They are unable to assess and quantify the risk and therefore make an appropriate judgement on that value of transferring it to the insurance market; and/or

2. They lack the required levels of cyber resilience that would make them insurable. There is therefore a clear need to educate these end clients to improve their knowledge of their own cyber exposures.

There can often be a disconnect within client organisations between chief information security officers (CISOs), who best understand cyber risk, and risk managers in specific finance functions, who are typically the buyers of insurance but who face challenges translating cyber risk into business risk. Given this situation, it is not surprising that the terms of coverage are often not fully understood within a single organisation, as proven by the large number of cyber claims that end in litigation.

To enable a more accurate assessment and quantification of cyber risk, and therefore make it easier for organisations to transfer their risks to the insurance market, two things need to happen:

1. Standards need to be introduced (via industry bodies or even regulators), at least at a regional level, to harmonise the language in relation to cyber losses. Not only would this facilitate increased incident-reporting, it would also enforce minimum requirements for both cybersecurity and cyber insurance.

2. Collaboration is required in the sharing of cyber incident data, not only between the public and private spheres but also between insurers and brokers, to create centralised and anonymised cyber incident data repositories.

Both of these developments will give insurers and cybersecurity professionals access to the data that they need to better assess cyber risk and increase the amount of cyber insurance coverage currently being offered as a result. End client education of cyber risk through clear and consistent communication supported by relevant data is another critical element.

Developing an end-to-end view

MOVING FROM RISK INDEMNIFICATION TO HOLISTIC PROTECTION

How then can insurers and brokers grow their cyber books sustainably? When developing cyber propositions, a holistic view of end clients' cyber protection needs to be taken in collaboration with partners in the wider cyber ecosystem. Rather than focusing on the pure indemnification of cyber risk. As outlined below, sound risk assessment, mitigation and incident management should form an integral part of any risk transfer solution.

Cyber insurance propositions based on this more holistic view can create a virtuous circle for clients and insurers (see Figure 2). By assessing clients' risks more accurately; helping them to better understand them; providing more relevant risk mitigation advice; and encouraging the actioning of these mitigations through better policy wordings, insurers can help clients reduce the likelihood of a successful cyber-attack. This, in turn, makes clients more attractive risks to insure, enabling the circle to start again.

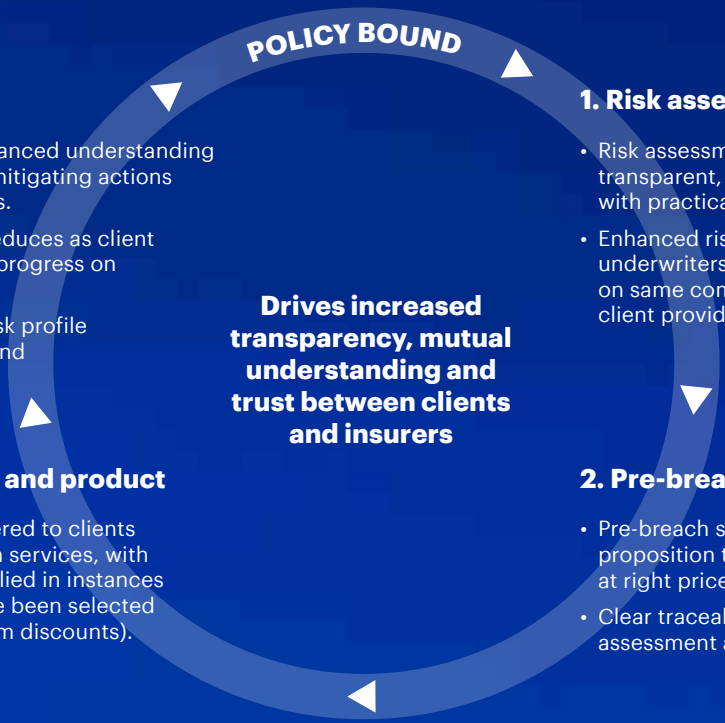
There are four key components of this process: risk assessment, risk mitigation, risk transfer and incident response.

Risk assessment to enhance transparency

An accurate and complete assessment of cyber risk, communicated transparently to the end client, is vital. Insurers and brokers can work together to provide value-added services that help end clients become better educated on their cyber risks in a way that creates mutual understanding on the relevant risk factors and exposure. This includes:

- **Threat intelligence:** Developing an understanding of the evolving threat actor landscape targeting the industry and sector. Leading underwriters can incorporate both industry-specific and company-specific threat intelligence into the core underwriting decision.
- **Strengthening industry-specific cyber-risk frameworks and assets:** Underwriters should develop industry specialisations for cyber, to gain a deeper understanding of end clients' value chains, technology architectures and key cyber-risk factors.
- **Client training, thought leadership and webinars:** Providing value-added services to inform clients, including through digital media, will further help to address the education and knowledge gap.

Figure 2: A 'virtuous circle' for cyber insurance



1. Risk assessment

- Risk assessment for client is more transparent, relevant and accompanied with practical risk mitigation advice.
- Enhanced risk assessment tools enable underwriters to better assess risk, based on same common set of information client provides.

2. Pre-breach services

- Pre-breach services are integrated into proposition to clients (e.g. as bundles at right price point).
- Clear traceability between risk assessment and pre-breach services.

3. Tailored coverage and product

- Coverage and terms offered to clients are related to pre-breach services, with preferable wordings applied in instances pre-breach services have been selected (ultimately, even premium discounts).

4. Better risks

- Client benefits from enhanced understanding of own risk profile, and mitigating actions from pre-breach services.
- Insurer s risk exposure reduces as client continues to renew and progress on virtuous circle.
- Understanding of true risk profile is enhanced, with trust and transparency increased.

Drives increased transparency, mutual understanding and trust between clients and insurers

Source: Accenture analysis

Pre-breach services to support risk mitigation

Pre-breach risk mitigation services—provided either by brokers, insurers or the extended cybersecurity ecosystem—should be part of the core proposition. These will foster a risk-engineering-focused mindset, and help end clients reduce their risk exposure. These include:

- **Ongoing threat monitoring:** Leading insurers will start to provide ongoing pre-emptive threat intelligence to bound clients, for example, by informing them in near-real time of company-specific threats on the dark web. Providing this communication throughout the policy lifecycle—rather than once a year at renewal—will help to build mutual transparency and trust, ultimately improving retention and client risk profiles.
- **Targeted risk mitigation advice aligned to risk assessments:** Risk mitigation advice, based on the client's own risk self-assessment, should be geared to each specific client. The proposition should also include more extensive pre-breach services, such as internal network cyber diagnostics, incident response contingency planning and coached incident simulation.

Risk transfer through tailored coverage and products

The core risk transfer offering should be tightly coupled and aligned with risk assessment and risk mitigation products:

- **Cover and premiums:** Clients' more accurate risk assessments and implementation of the relevant risk mitigations could be rewarded with improved terms, and ultimately more risk-aligned premiums. Even poorer risks declined as being outside the current risk appetite could be coached with a set of clear risk mitigations, such as existing minimum standards, which—if actioned—might lead to cover being offered.

Breach response support to achieve better risks

Insurers' cyber claims services are vitally important to end clients, because at the point of 'first notification of loss', the incident being reported may well be an ongoing, live, time-critical security breach that requires management and remediation. An effective post-breach capability will then be key in restoring the client to a pre-incident state in a speedy and cost-effective way. Those insurers that deliver this will ultimately be rewarded with lower claims and costs.

- **Flexible and scalable incident response:** Insurers' incident response capabilities must be flexible and scalable to ensure the aggregation risk is in line with their ability to respond. For example, if a downstream supplier is disabled, impacting many different companies across different industries, can the insurer respond adequately?

- **Partners across the value chain:** Effective incident response requires coordination across a wide range of third parties, including law firms (to notify relevant regulatory bodies), IT forensic firms (to investigate causes and remedy the breach) and PR firms (for managing communications and reputational impacts). Insurers must provide the end-to-end 'glue' to hold these services together, delivering for the client in a moment of peril.

- **Global, reliable and accessible:** Insurers writing cyber business globally will need a cyber claim response capability that is global (multi-lingual), consistent and accessible through 24x7 call centres and using mobile apps to support claimants.

Moving beyond a risk transfer mindset is key

To develop this marketplace, insurers will need to move beyond the traditional risk transfer mindset, and develop cyber propositions that incorporate all four of these elements to deliver end-to-end protection. Executing this will not be easy, and will require insurers to seek out new partners, upgrade their own capabilities and develop a new generation of products with components they've never offered before. However, the effort will be justified by the rewards: capturing a major new source of profitable revenue growth.

Why London has the global edge as a cyber insurance centre

The London Market is already firmly established as a global leader in underwriting cyber insurance policies. In Accenture's view, London will retain and strengthen this position through its leadership in four key dimensions.

1. AN UNRIVALLED CONCENTRATION OF CYBER PLAYERS AND TALENT

London's thriving services sector combines all the elements needed for a world-class cybersecurity ecosystem. It is home to some of the world's leading cyber legal firms and cyber litigation experts; a thriving InsurTech and cyber resilience start-up community, which is breaking new ground in areas like blockchain security and biometric identification; large-scale security consulting firms offering a plethora of cyber resilience services; and—of course—the innovative underwriting pioneered by the London Market. All of which is underpinned by the flexibility that Lloyd's subscription based model provides and supported by the vast number of insurers and brokers operating in the City. Recent developments include the launch of the London Cyber Innovation Centre to act as an innovation incubation space for cyber start-ups. This ecosystem provides an ideal environment in which to meet all of a client's required cyber protection.

This physical concentration of companies and people also means that London is able to address one of the core challenges in the cyber space: the war for security talent. While large financial institutions generally have strong security capabilities—either in-house or through outsourcing—which enable them to assess and manage cyber risks effectively, this is far less true for mid-market businesses and SMEs, which struggle to recruit or access the necessary talent.

Underwriters and brokers will need to build and grow specialist cyber teams to help shape the next generation of cyber insurance "products, understand the evolving nature of the threats and risks, and tap into new segments such as SMEs. The scale of the London Market offers unrivalled opportunities to find, recruit and develop insurance professionals with the necessary cyber skills, thereby adding to many of the world's leading experts already here. The UK also has a ready-made supply of non-insurance cyber professionals, together with the educational and industrial infrastructure and facilities required to grow this workforce quickly. For example, there are approximately 800 specialist information security firms and 14 centres of excellence in cyber defence located in the UK alone.

2. OPERATING WITH A GLOBAL MINDSET AND SCALE

Cyber is a peril that is global in nature. Threat actors such as nation states operate on the global stage, and a vulnerability in a popular technology platform could expose firms to the same risk worldwide. Given these characteristics, global underwriting centres such as London tend to have an edge over their local counterparts due to the economies of scale inherent in understanding the threat actors, vulnerabilities and resulting risks. Growth in cyber lines will also be partly driven by cross-selling cyber extensions into more mature lines of business already underwritten on a global basis through the London Market, such as property and casualty (P&C).

More generally, London and the UK are renowned across the world for their cybersecurity expertise. Examples include the GCHQ monitoring centre, the UK Government's National Cyber Security Strategy, and the London Metropolitan Police's success in selling cyber services to law enforcement agencies in other countries. Overall, the UK is a 'top-five cyber nation' that already exports about £1.5 billion of cyber products and services annually to customers worldwide.[20]

Threat actors such as nation states operate on the global stage, and a vulnerability in a popular technology platform could expose firms to the same risk worldwide.

3. UNDERPINNED BY LEADING MARKET INFRASTRUCTURE, AND ROBUST LEGAL AND REGULATORY FRAMEWORKS

The UK's regulatory system is an advantage, supported by the UK's transparent and globally-respected legal system. The Prudential Regulation Authority (PRA)—the body through which the Bank of England regulates and supervises financial services firms—has a strong global reputation that inspires confidence, and is including cyber as a key element of its 2019 UK insurance stress testing exercise. This solid regulatory base may become even more important, given the structural changes cyber insurance is currently going through, as reflected by the frequent test cases to determine the extent of cyber insurance liability and coverage.

> **We've seen that the scarcity of cyber data and accumulative nature of the risks are key challenges for underwriters looking to understand cyber exposures.**

4. SUPPORTED BY THE RELEVANT DATA AND THE LATEST ANALYTICS

We've seen that the scarcity of cyber data and accumulative nature of the risks are key challenges for underwriters looking to understand cyber exposures. To overcome this lack of data, it is vital for the insurance industry, information security providers and other participants to come together and share information in a collaborative manner, supported by cutting-edge analytical techniques such as deep learning and natural language processing (for example, of dark web threat data). These types of consortiums and data-sharing initiatives are most likely to form in markets where there is a high concentration of expertise, and a long history of mutual trust.

The London insurance market is second to none in all of these respects, and institutions such as the City of London Corporation, the Association of British Insurers (ABI), Lloyd's of London, and the London Market Group (LMG) are well placed to play an active role in defining common standards and approaches, supported by many of the world's most advanced technology, data and analytics firms. The ready availability of these technologies helps insurers apply analytics to gain the fullest possible insight and value from pools of shared data, and quantify and price cyber risk more accurately.

Conclusion: It's time to act together

Meeting clients' cyber insurance needs presents one of the biggest opportunities currently on offer in the global insurance market. Despite the significant challenges insurers face in realising it, those who focus on clients' end-to-end protection needs can develop winning propositions in this fast-emerging area.

This will require them to extend out into a wider ecosystem of cybersecurity players. Insurers who fail to do this will end up writing business without understanding the full nature of the end risks, will attract those clients who are susceptible, and will not develop bespoke pricing capabilities. These factors will make them ultimately vulnerable to 'black swan'-type events that could incur potentially catastrophic losses.

So the stakes are indeed high. And those insurers who are committed to succeeding in this space will benefit from leveraging the London Market. In addition to its strength, reputation and depth as a provider of indemnification, London has a wider cybersecurity ecosystem that provides precisely the environment insurers need to develop market leading cyber 'protection' propositions. Insurers can therefore continue to play a critical role in supporting the cyber resiliency of their clients and, in doing so, London will further enhance its position as a genuine centre of cyber excellence.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions underpinned by the world's largest delivery network Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

REFERENCES

1 Munichre.com. (2018). Excel. Grow. Invent. [online] Available at: https://www.munichre.com/site/corporate/get/documents E 493166974/mr/assetpool.shared/Documents/0 Corporate Website/6 Media Relations/Press Releases/2018/MunichRe Presentation Baden Baden 2018.pdf

2 McAfee and The Center for Strategic and International Studies (CSIS). Economic Impact of Cybercrime No Slowing Down. [online] Available at: https://csis prod.s3.amazonaws.com/s3fs public/publication/economic impact cybercrime.pdf

3 Accenture.com. (2019). 2019 Cost of Cybercrime Study | Accenture. [online] Available at: https://www.accenture.com/gb en/insights/security/cost cybercrime study.

4 Turturro, J. (2019). Cyber Review: Understating risk in an evolving threat landscape | JLT Re. [online] Jltre.com. Available at: https://www.jltre.com/our insights/publications/catastrophe year in review 2018/cyber review

5 Accenture.com. (2019). State of Cyber Resilience Index 2018 | Accenture. [online] Available at: https://www.accenture.com/gb en/insights/security/2018 state of cyber resilience index

6 McAfee and The Center for Strategic and International Studies (CSIS). Economic Impact of Cybercrime No Slowing Down. [online] Available at: https://csis prod.s3.amazonaws.com/s3fs public/publication/economic impact cybercrime.pdf

7 Accenture.com. (2019). The Cost of Cyber Crime. [online] Available at: https://www.accenture.com/ acnmedia/PDF 96/Accenture 2019 Cost of Cybercrime Study Final.pdf#zoom 50 [Accessed 9 May 2019].

8 Ninth Annual Cost of Cybercrime Study. (2019). Accenture. https://www.accenture.com/ acnmedia/PDF 96/Accenture 2019 Cost of Cybercrime Study Final.pdf#zoom 50

9 Crypto money-laundering. (2018, April 26). The Economist. https://www.economist.com/finance and economics/2018/04/26/crypto money laundering

10 Brandom, R. (2019, January 9). Why the Ethereum Classic hack is a bad omen for the blockchain. Verge. https://www.theverge.com/2019/1/9/18174407/ethereum classic hack 51 percent attack double spend crypto

11 Brundage, et al. (2018, February). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

12 Swiss Re Institute: Sigma - Commercial insurance: innovating to expand the scope of insurability No5 / 2017

13 Aon.com. (2017). Global Cyber Market Overview. [online] Available at: https://www.aon.com/inpoint/bin/pdfs/white papers/Cyber.pdf

14 Agcs.allianz.com. (2015). A Guide to Cyber Risk. [online] Available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS Cyberrisk report.pdf [Accessed 7 May 2019].

15 Advisenltd.com. (2018). The European cyber insurance market: ready for growth, but will it overtake the U.S.? - Advisen Ltd. [online] Available at: https://www.advisenltd.com/the european cyber insurance market ready for growth but will it overtake the u s/

16 Accenture.com. (2017). Insuring Autonomous Vehicles: An $81 Billion Opportunity by 2025. [online] Available at: https://www.accenture.com/ acnmedia/PDF 60/Accenture Insurance Autonomous Vehicles PoV.pdf

17 Oecd.org. (2017). Global Insurance Market Trends. [online] Available at: https://www.oecd.org/daf/fin/insurance/Global Insurance Market Trends 2017.pdf

18 Accenture.com. (2018). Cyber Threatscape Report 2018. [online] Available at: https://www.accenture.com/ acnmedia/PDF-83/Accenture Cyber Threatscape Report 2018.pdf

19 Partnerre.com. (2018). 2018 Survey of Cyber Insurance Market Trends. [online] Available at: https://partnerre.com/wp content/uploads/2018/10/2018 Survey of Cyber Insurance Market Trends.pdf

20 Source: https://www.gov.uk/government/news/government announces support for cyber security companies to protect-uk-and-allies

www.accenture.com

Accenture

@Accenture

190612