CITY OF LONDON

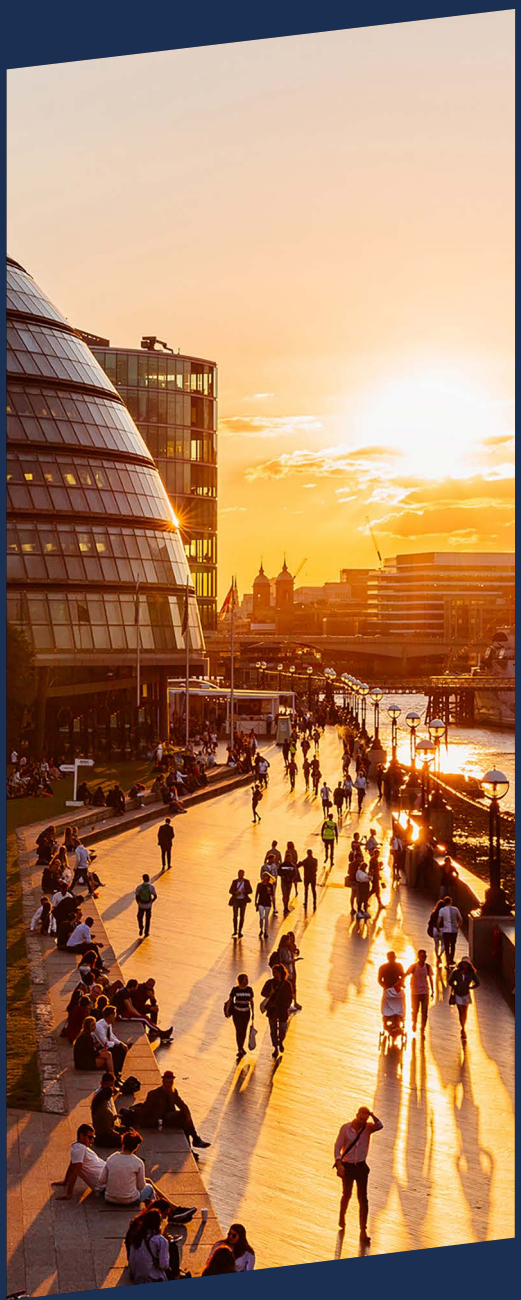
THE GLOBAL CITY

In association with

accenture

The future of cyber insurance

Next steps for the London Market



Foreword

On the behalf of the City of London Corporation and associated industry stakeholders, I am very pleased to introduce this report on the "The future of cyber insurance—next steps for the London Market".

Catherine McGuinness
Chair of Policy,
the City of London Corporation

On behalf of the City of London Corporation and associated industry stakeholders, I am very pleased to introduce this report on the "The Future of Cyber Insurance - Next Steps for the London Market".

Needless to say, 2020 has been a tumultuous year. The pandemic has driven a marked acceleration in businesses adopting digital and cloud technologies, as they look to support their remote workforces through this time and adapt to a more virtual environment. Consequently, the importance of proper cyber security for both business and individuals is ever increasing, and cyber insurance plays a role in helping meet this challenge.

In this report, we highlight the City of London's globally unique position as both a hub for commercial insurance, as well as the centre of a thriving and comprehensive ecosystem of cyber security service providers. No other city has London's concentration of (re)insurers and brokers, co-located with some of the world's leading cyber security service providers spanning across insuretech start-ups, large cyber technology vendors and specialist cyber law practices.

As part of supporting London's re-emergence from the pandemic, we believe the City of London Corporation can play an important role co-ordinating cross industry stakeholders, to further promote London's role as a global cyber insurance hub. In addition to the economic benefits, this will improve the cyber resiliency of UK businesses more broadly– ultimately helping keep us all more cyber secure.

I am therefore pleased to introduce this report that describes how we might do this, and I would like to add a special word of thanks to senior members who contributed. In particular I want to acknowledge the contributions of Alderman Bronek Masojada, Alderwoman Susan Langley and Dominic Christian, both to this report and the modernisation of the London Market more generally.

Together we are excited about the opportunity to contribute to the next phase of growth of the cyber insurance market in London.

Kind Regards

Catherine McGuinness
Chair of Policy,
the City of London Corporation

Introduction

The Covid-19 pandemic has accelerated technology transformation across all industries and entrenched the structural shift from the physical to digital. The risks of cyber attack, already significant pre-pandemic, now stands as one of the greatest risks to the world economy and the 'new normal' of post pandemic life.

The purchase of cyber insurance, transferring the risk of damage or loss from cyber attacks to a 3rd party insurer, is an increasingly popular part of a company's overall strategy in managing the risk of cyber threats. The London Market has emerged as one of the key global players for writing cyber insurance, with approximately a quarter of global cyber premiums written through the Lloyd's market.[1]

It is estimated that the total value of the global economy at risk due to cyber-crime is expected to be $5.2 trillion over the next 5 years,[2] and the current crisis will only add to the momentum behind the increase in cyber-crime and its costs. The decentralisation of workforces and business pose difficulties to existing security regimes which will require adapting to the new post-Covid normal. Many employees have no new security guidance, no new training, and no new tools to secure their personal laptops if they are used for work purposes.[3] As business activities transition to unexplored and less secure territory, the importance and relevance of insurance in cyber security will only intensify.

Cyber insurance on its own is not a sufficient strategy for a company responding to cyber attacks. Rather, it should be one critical part in a wider cyber resiliency framework, which also includes preventative actions to reduce cyber vulnerabilities; pro-active identification of cyber threats; and preparation of response plans for when cyber incidents occur.

To execute this broader cyber resiliency strategy, companies must work within a wider cyber security ecosystem, outside of the insurance market, which includes cyber security vendors, incident response providers and cyber specialist law firms among others. Such a cyber security ecosystem is very vibrant and mature within London.

This co-location in London of both a leading cyber insurance market, as well as a thriving cyber security ecosystem provides an opportunity for London to further enhance its position as a global cyber insurance hub, and thus benefit from the strong growth potential of the global cyber insurance market.[4]

In order to fully grasp this opportunity however, London must overcome a set of challenges inherent in the cyber insurance business. This will require the London cyber security ecosystem and insurance market to come together and set a clear vision for London as a cyber insurance hub, as well as develop a programme of activity to drive forward further development of the cyber insurance market.

London, then, has an opportunity to develop into the pre-eminent global cyber protection hub—both serving globally as a hub for writing cyber insurance and offering associated protection services, but also playing a pivotal role in the cyber protection of UK PLC in our post Covid landscape.

1. London as a cyber insurance centre

London has a compelling set of strengths as a cyber insurance centre, driven in part by the co-location of an insurance ecosystem (providing underwriting expertise, innovation, capital, market infrastructure and prudent regulation) and a cyber security ecosystem (providing broad range of technical cyber security services, incident response, cyber specialist law firms, PR firms).[5]

These two elements—an insurance market and a cyber security ecosystem—makes London unique globally. Despite the accelerated shift from virtual to physical working from the pandemic, these elements of shared physical location remain important. Office based roles will remain for many, and existing networks of shared relationships and specialist knowledge will endure. In addition, London based firms will continue to operate in a common legal and regulatory framework, under a common working culture—even if that now incorporates more virtual interaction than previously.

This 'extended cyber' ecosystem provides numerous advantages for cyber insurers and brokers in London. Insurers can partner with cyber security technology vendors to develop new value-added services for clients (focused on preventative measures such as pre-emptive threat intelligence); as well as access expertise on emerging technology areas such as blockchain and AI. They can access a wider talent pool of cyber literate employees; high quality legal and PR support; and benefit from a forward looking and cyber aware regulator and government policy.

London is the only location that combines a global insurance hub with a leading technology ecosystem providing comprehensive services for cyber security.

Silicon Valley is a global leader in technology, and Hartford, Connecticut, boasts a concentration of top insurers, but the potential of a combined cyber insurance hub in North America is diluted by geographical distance. The most obvious candidates for cities which combine a significant insurance presence with a leading cyber security ecosystem are New York and San Francisco; although both these centres are US focused rather than global. Other leading insurance centres – such as Bermuda, Zurich, Hong Kong, Dubai, Tokyo, Shanghai, lack the cyber security ecosystem on the scale present in London. And of the leading global cyber security areas, such as Tel Aviv, the San Francisco Bay Area, Washington DC, Singapore, Shenzhen, none of these locations have the scale of the insurance market that is present in London.

> “London then is the only location that could truly claim to be both a leading global insurance market, as well as a world leader in cyber security—and this gives it a huge competitive advantage.

2. Challenges for growth

Whilst London enjoys a positive set of factors that make it an attractive market for writing cyber insurance, it cannot afford to be complacent in the race to capture future market growth.[6] It must compete globally with other emerging hubs to earn this business and status, as well as help address some of the wider challenges in the cyber insurance market.

A genuinely global cyber insurance market

As cyber capabilities grow and mature, cyber insurance is likely to be used as a last line of protection for organisations.

Cyber security protection costs have risen in past years and continue to rise with 69% of business leaders saying that staying ahead of attackers is a constant battle and the costs are unsustainable.[7] This trend is unlikely to change as the digitalisation of workforces and infrastructures accelerates in the wake of Covid-19. Cyber security programmes only directly protect about 60% of an organisation's business ecosystem with the other 40% stemming from indirect attacks on the wider environment such as third-party suppliers.[8] There is a clear gap for risk mitigation and transfer for cyber insurers to fill. The cyber insurance market itself is seeing rates rise significantly, as insurers look to price in the growing risk of threats such as ransomware.

Growth in the cyber insurance market is forecast to continue, yet this will not stem primarily from already mature cyber markets such as the US, which the London Market traditionally supports well. Instead emerging regional markets in mainland Europe, APAC and LATAM will be key drivers of growth. An obvious difficulty will be that these markets may have less historic connection to the London Market, preferring to place business locally. Making London the natural location for providing these clients with cyber insurance will require proactive outreach from insurers and brokers.

In addition, global competition to capture a larger share of the cyber insurance market is increasing. Numerous locations, across the US, Europe, APAC and LATAM, are actively promoting initiatives and policies to foster the growth of cyber security services, including insurance. For instance, the New York Economic Development Corporation announced in October 2018 a $100m initiative to 'transform New York City into a global leader of cyber security innovation and talent'.[9] Coupled with New York's strength in Financial Services, such an effort could certainly further enhance a cyber ecosystem to rival London's.

There is evidence of similar market stimulation activities in emerging cyber markets also. Singapore for example, has committed to creating the world-first commercial cyber risk pool, with the Singapore government working to bring together 20 insurers to create up to US$1 billion in capacity and provide bespoke cyber coverage—with the overall aim of creating greater cyber resiliency in Singapore and beyond.

Growth of cyber insurance in London then, will depend on how well the London Market can engage with these newer emerging markets, and fight off competition from other regional hubs through superior cyber products and services.

> "Cyber security protection costs have risen in past years and continue to rise with 69% of business leaders saying that staying ahead of attackers is a constant battle and the costs are unsustainable.[7]

Challenges in the wider cyber insurance market

In addition to the regional dynamics of the cyber market, there remain significant challenges at the market level as a whole that require resolution before the cyber insurance market can reach its full potential scale. For London to be a genuine leader in cyber insurance, it must aim to show leadership in solving these challenges also.

A lack of trust between cyber insurance providers, and end clients.

Some prospective buyers view the core cyber insurance product as not sufficiently transparent, with a lack of a clarity around what exact aspects of cyber risk are covered. Some clients themselves may be relatively unsophisticated cyber insurance buyers, who are unclear as to what are the cyber threats they are trying to counter, and the key cyber vulnerabilities their businesses have. Furthermore, there is a perception, reinforced by media coverage, that even if cover is purchased insurers may not pay out on cyber policies in the event of large-scale incidents.

The most notable example of this public debate on the reliability of cyber policies is the widely reported fallout from the 2017 Not Petya attack. In this incident, a ransomware attack crippled several companies, causing over $100m of damages primarily from business interruption losses. Following the findings by US & UK governmental agencies that Russian military were 'almost certainly' behind the attack,[10] one insurer attempted to deny a claim for damages under the policy, due to a war exclusion clause i.e. cyber damages from war like acts involving nation state actors were specifically excluded from the policy. While the policy in question was not a standalone cyber policy, but an all risks property policy and the case continues to play out in Illinois state courts in the US, the dispute was seen as a test instance for the wider cyber market as to whether cyber insurers would genuinely pay out in cases of cyber incidents.

The Covid-19 pandemic is exacerbating this trust gap between insurers and claimants, recently demonstrated by the Financial Conduct Authority intervening on behalf of thousands of companies seeking business interruption pay outs refused by insurers. The complex and unpredictable nature of cyber risks not only pose difficulties for insurers underwriting the risks but also to insureds who may not have full confidence that they will receive compensation after an attack. This doubt may undermine the clear business need for cyber insurance in the market.

Such examples are evidence of a 'trust gap' between cyber insurers and end clients. Insurers may need to work harder to clarify the exact scope of their risk transfer product and match it to client needs, while the wider market needs to support improved client education on how cyber insurance can support a company's wider cyber resiliency.

> "Some prospective buyers view the core cyber insurance product as not sufficiently transparent, with a lack of a clarity around what exact aspects of cyber risk are covered.

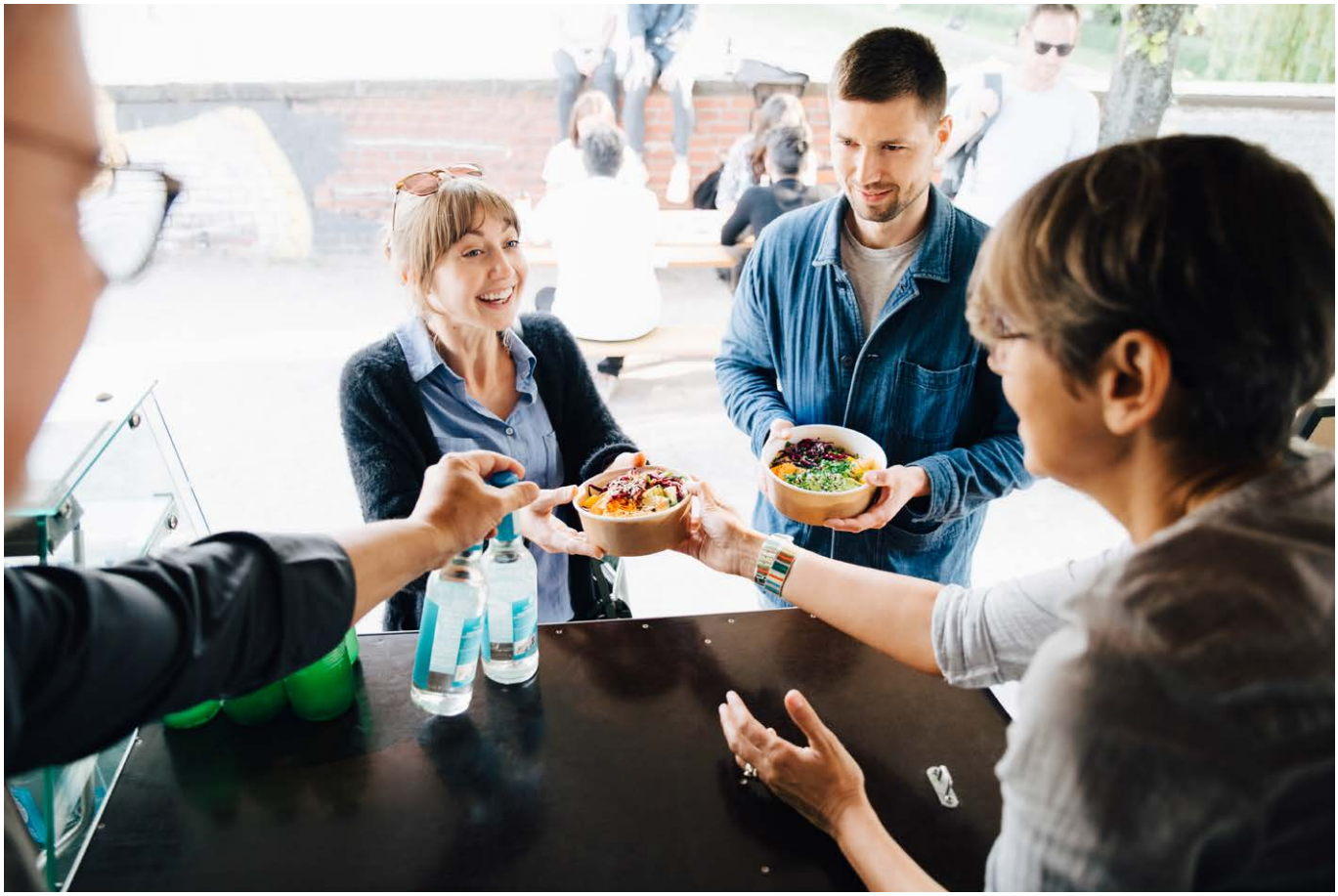
Limited adoption of cyber standards inhibits preventative measures.

The cyber insurance industry lacks the kind of widescale adoption of an established set of security standards that would be considered routine for more traditional risks such as property and motor. The set of safety standards that have evolved over time in these markets (e.g. Thatcham standards in motor) provide an industry-wide language that enables consistency in evaluating risk; and support the market pooling of a consistent set of risk and claims data to further develop more accurate pricing. Standards are also important in providing insurers with clear guidelines on when to encourage clients to take preventative measures if they do not meet required standards.

In the case of cyber risk, while numerous cyber security standards exist (for example, the UK's Cyber Essentials scheme aimed at SME businesses; through to NIST/ISO/CIS standards for larger corporates in particular industries), the rapidly evolving nature of the technology and threat, as well as the limited time in which cyber insurance has been on the market, has meant that these standards lack widescale adoption by end clients, and are not consistently used or promoted by insurers. Conversely, standard regimes that are too rigid, or generic, fail to adequately assess and mitigate risk and collapse into box ticking exercises.

Ultimately, this lack of common standard adoption hinders the growth of the cyber market, clients are not incentivised to adopt preventative measures, nor insurers to offer them; the market is unable to collectively share data or assess risk on a consistent basis; and the cyber product and associated services are unable to evolve to meet genuine client needs.

3. Three focus areas for the London Market



What is the right way for London to overcome these challenges, to fully leverage the power of the combined insurance and cyber security ecosystem and capture greater share of the global cyber insurance market? We suggest below several areas of focus.

Emerging stronger and showcasing London.

Countries across the world are in the process of relaunching their economies as they face into a pandemic induced dip; the UK, and London within it, is no different. The economic slowdown due to Covid-19 may mean a short-term decrease in discretionary spending which may impact the uptake of cyber insurance. However, the long-term strategic importance of cyber resiliency and protection will remain, and the City of London should be primed to anticipate this upcoming demand.

Attracting business from emerging cyber insurance markets requires engagement and outreach to these regions to articulate the benefits of placing business in London. A clear, precise guiding vision for the market, positioning London as a cyber insurance centre and articulating the benefits associated with this, would support this regional engagement, and set the market direction for London. Created through coordination and consultation with a cross market set of stakeholders, it would articulate an appropriate level of ambition for the market (e.g. in terms of share of total global Cyber Gross Written Premium (GWP)).

Underpinned by this vision, and with an objective of showcasing London's strength as a cyber insurance centre, there is an opportunity to launch a centrally coordinated marketing campaign for London as a cyber hub. Such a campaign could showcase some of the unique features of the London cyber insurance market. It would focus on targeting some of the emerging cyber insurance markets such as APAC / LATAM, with the intended audience both local players in the insurance market (carriers and brokers), as well as representatives in end client organisations (risk managers purchasing cyber insurance, as well as CISO's).

Future market growth will come both from the traditional cyber buyers such as large corporates; but also increasingly from mid market and SME businesses around the globe purchasing cyber for the first time. Becoming a genuine cyber insurance hub then, will depend on creating an insurance market that can service a fuller spectrum of client need (from large corporate to SME), with an ease of access and low cost to serve.

> "Attracting business from emerging cyber insurance markets requires engagement and outreach to these regions to articulate the benefits of placing business in London.

Take the lead in setting standards and sharing data to help shape the global cyber market.

There is an opportunity for a cross-market effort, driven out of London, to determine and promote the adoption of relevant cyber security standards that will underpin cyber insurance products. In particular, the appropriate set of standards for various market segments, from SMEs to multinationals, and for addressing various cyber risk factors (e.g. infrastructure vulnerabilities, data privacy controls) can be identified and embedded into insurance products.

A significant amount work has already been undertaken by the UK Government and security industry to establish security standards and frameworks and these should be leveraged and appropriately right-sized based on market segment as part of this initiative. The National Cyber Security Centre (headquartered in London) already plays a proactive role in producing guidance for improving the cyber security of UK businesses. The numerous insurance market bodies, the London Market Association, British Insurance Brokers' Association (BIBA), AIMRIC representing risk managers and insurance buyers, can also make an important contribution.

In addition to this, the right incentive systems for market participants (insurers, clients, cyber security vendors) need to be defined centrally with the aim of increasing adoption. Insurers may need to use their collective power to introduce a set of minimum cyber security standards before cover is provided. Such standards will also support the improved transparency of the cyber product, helping to bridge the trust gap in the cyber market.

The development and adoption of cyber security standards would both enable and encourage greater levels of risk management and a greater level of data sharing between various market stakeholders; which in term would allow insurers to more accurately price and evaluate risk. Bodies such as the Information Commissioner Office (ICO), Lloyd's, insurers, brokers, cyber security vendors collaborating on a market wide data source would provide a more robust, comprehensive asset to leverage for pricing and underwriting, and support greater risk transfer from clients to insurers, helping address the underinsurance gap.

Supporting cyber resilience of UK PLC.

In the longer term, the cyber insurance market in the UK should play a pivotal role in the cyber protection of UK PLC. Currently, the Association of British Insurers estimates that less than £100 million of GWP written in the UK relates to UK cyber risk (compared to the domestic UK pet insurance market of more than £1.1 billion in size, ten times the size). Only 11% of small businesses in the UK have cyber insurance policies in place. This suggests the London cyber market needs to do more to support the cyber resiliency of the UK through supporting growth in the UK domestic cyber insurance market.

The UK has numerous geographical locations with strong cyber expertise that can play a role in the overall cyber security ecosystem. Outside of London, universities such as Oxford or Cambridge offer innovation environments for academic/private sector cyber collaborations; Cheltenham benefits from headquartering GCHQ, one of the world's leading cyber security government agencies; Belfast contains an emerging cluster of cyber security firms; and cyber security is a core part of the overall Northern Powerhouse strategy, with e.g. Manchester chosen as a new site location for GCHQ. The UK then has a wealth of regional cyber security capability and talent.

As relates to cyber insurance, the role of London may be to act as a 'hub' in a hub-and-spoke model, providing a central location of cyber insurance innovation and expertise (the 'hub'), focused on supporting global multinational clients through the London Markets - and working with other UK regional cyber security centres (the 'spokes') to disseminate that insurance expertise and promote the development and adoption of cyber insurance in those areas.

In such a way, London's success in capturing a greater share of the global cyber insurance market benefits the whole of the UK, through the sharing and exchange of knowledge with a series of UK regional cyber communities, ultimately contributing to the improved cyber resilience of UK businesses.

"

The UK has numerous geographical locations with strong cyber expertise that can play a role in the overall cyber security ecosystem.

4. Market coordination and conclusion

Stakeholder coordination.

We have seen that the unique strength of London lies in its extended cyber security and insurance ecosystem. How best then to take advantage of this strength, and further accelerate the evolution of London to a global cyber insurance hub?

Against the backdrop of Covid-19 and the structural business changes it has accelerated, the City of London should be ready to initiate at speed and at scale as the market recovers. While the co-located extended cyber ecosystem is London's greatest strength, it also presents its greatest challenge or how to align a diverse set of stakeholder groups, with multiple different priorities in a way to effectively benefit the cyber insurance market overall.

To fully leverage the strength of this ecosystem there must be co-ordination across it or to help define a shared vision, to encourage the partnership between public and private sector, to bring together competing insurers and carriers, and to align the insurance and cyber security industries. In executing on the focus areas described in Section 3, engagement with and participation from numerous stakeholder groups are critical.

Most obviously, support from the wider insurance market is fundamental. Aligning any initiatives to develop the cyber insurance market with the wider insurance transformation of the market requires support from Lloyd's, as well as associated bodies such as the London Market Group. Any attempt to develop cyber standards, or pool market data, will be dependent on outreach to individual carriers and brokers. Initiatives that promote wider penetration of cyber insurance into the SME segment (and even into consumer products) will benefit from engagement with the Association of British Insurers.

Alignment and support would also be required from numerous governmental bodies. Consumer regulatory bodies such as the ICO and FCA may play a role in supporting the improved transparency between insured and insurer in the cyber market and clarifying the protections individuals and companies require. The proposed UK Cyber Security Council, to be designed and delivered by the Institute for Engineering Technology (IET), will support the wider objectives of building up the cyber security talent pool in the UK. Deep pools of cyber expertise in exist in GCHQ and the National Cyber Security Centre. Engagement with the cyber specialist law enforcement teams, such as the City of London Cyber Police, will also be required.

The final stakeholder group is the cyber security ecosystem—the technology vendors, the deep specialist cyber security providers, incident responders, breach coaches and specialist cyber legal firms, PR firms, cyber-focused analytics and data providers, forensic accountants, and others. All these firms have a part to play in supporting the end cyber protection and cyber resilience of insured clients.

City of London Corporation

As the custodians of the Square Mile in which many of these stakeholders are based, the City of London Corporation has an opportunity to play an important role in this market coordination, and successfully executing on the vision of establishing London as the premier global cyber insurance market.

Any initiative designed to further London as a global cyber insurance market should not be driven exclusively by only one of the above stakeholder groups in isolation from the others e.g. driven purely from within the insurance industry. Such an approach risks not fully capturing the benefits inherent in leveraging the wider cyber ecosystem. Instead, the City of London Corporation could be able to jointly engage the various stakeholder groups without a particular industry slant or bias to unduly influence the agenda. It stands uniquely placed in its ability to engage with the diverse public and private bodies in the cyber security ecosystem, who are in the most part united by nature of their physical co-location in the City.

Furthermore, the purpose for promotion of London as cyber centre should be kept in mind—ultimately, to support the growth of financial services in London, with a broader positive effect of promoting the UK economy and contributing to the improved cyber resiliency for UK companies. This aligns closely with the aims of the City of London Corporation, rather than these objectives being entrusted to a single one of the industry groups with differing agendas and commercial priorities.

Finally then—what precisely might this coordination role entail? It would involve support for the initial mobilisation of a wider programme—engaging with industry to determine appropriate executive sponsors, developing a governance structure for the programme. It would drive sponsor market engagement across the diverse stakeholder groups, helping bring together participants from the insurance market, the cyber security ecosystem and public sector. It would support the development of an appropriate vision for the City of London as a global cyber insurance hub, and foster support and alignment around that vision. Finally, it may also facilitate the transition to a series of working groups, focused on addressing particular challenges (e.g. the sharing of market data).

> “
>
> With such market wide coordination, London could leverage the full potential inherent in its cybersecurity and insurance ecosystems. Doing so would cement London’s reputation as a leading cyber insurance centre—writing a significant share of global cyber premium, and also playing a crucial role in the UK’s overall cyber resiliency strategy.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 506,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

References

1 Lloyd's Annual Report, 2018

2 Ninth Annual Cost of Cybercrime Study, 2019, Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

3 IBM, 2020. https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk

4 Current global cyber insurance GWP of c. $4bn in 2019, estimated to grow to c. $20bn GWP in 2025 - 2030, Figures based on internal Accenture Research

5 Cf. Inga Beale June 2019 "If we can connect the tech sector, the security sector and the insurance sector, [the UK has] got an unrivalled package to go out and cement our place as the leading centre for people to come for [these services].", https://tech.newstatesman.com/security/infosec-2019-lloyds-london-inga-beale

6 Note that the discussion of the challenges below is informed in part by the City of London sponsored Panel Discussion following the launch of the original report 'The Global Future of Cyber Insurance—and the London Market's Pivotal Role'

7 State of Cybersecurity Report 2020 https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

8 Ibid

9 cf. https://edc.nyc/press-release/nycedc-unveils-global-cyber-center-innovation-hub-and-new-talent-pipelines-secure-nyc

10 For example, see https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

Published by:

CITY OF LONDON

THE GLOBAL CITY

theglobalcity.uk

In association with

accenture