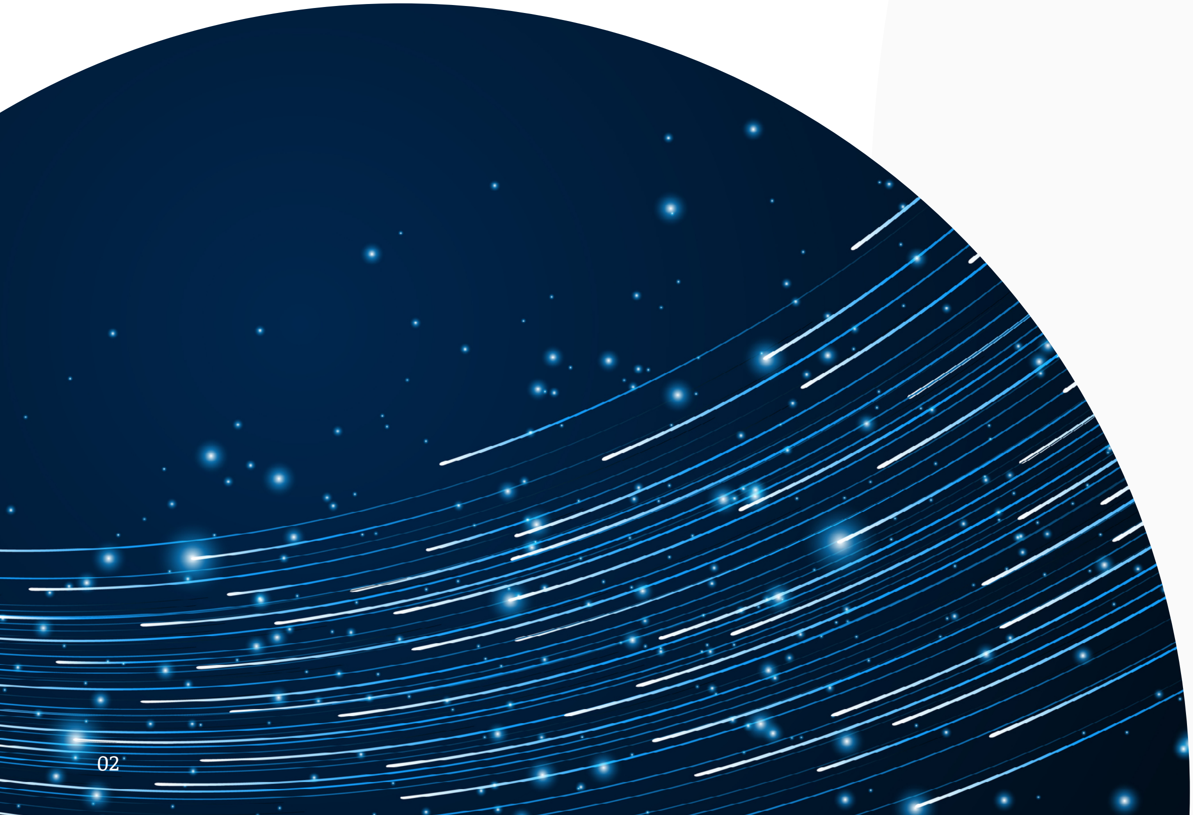
Bishopsgate

Cyber landscape 2024

Overarching trends

- Average cost of a data breach is now $4.45m, a 15% increase over three years.
- In a recent study, UK business leaders identified potential cyber-attacks as the largest threat to growth.
- Among S&P companies, 87% of balance sheet assets are intangible. Examples include intellectual property and personal information records, and these are frequently targeted by cyber criminals.
- Cyber crime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015.
- Adequate levels of cyber insurance are now deemed a standard client expectation across most industries.
- 560,000 new pieces of malware are detected every day.



Trends in the landscape

Ransomware

- Global cyber-attacks rose by 7% in Q1 2023 compared to the same period last year.
- As of 2023, over 72% of businesses worldwide were affected by ransomware attacks. This figure represents an increase from the previous five years.
- Ransomware attacks increased by over 37% in 2023, with an average ransom demand of $5.3m.
- It is expected that ransomware damage costs could exceed $265 billion annually by 2031.
- 20% of all current cyber-attacks are classified as ransomware.

Nation state attacks

- Russia & North Korea have been responsible for some of the most high-profile attacks in recent years.
- Cyber-attacks have become a key weapon in modern warfare, with nations targeting infrastructure, supply chains and networks.
- In Q1 of 2023, China was responsible for 79% of nation state cyber-attacks. North Korea, Russia, Iran and Pakistan made up the remainder of attacks.

Social engineering / business email compromise

Characterised by criminals deceiving their victim(s) to subsequently defraud an organisation, criminals will often hide behind seemingly legitimate digital infrastructure.

- This form of attack is increasing in its sophistication, and recently has been seen to by-pass multi-factor authentication.
- Email thread hijacking has resulted in a significantly higher click-rate on malicious links.

Supply chain attacks

Supply chain cyber-attacks are incidents in which a vulnerability or weakness in a third-party supplier's system is exploited to gain access to a company's data or systems.

- There is an increasing awareness that no business is immune from cyber-attack. All businesses face a risk of collateral damage from a supply chain issue, irrespective of the fact that they may not have been a specifically identified target. Recent software outages of this nature include Kaseya, Accellion and SolarWinds.
- Software supply chain attacks are expected to increase in both frequency and severity in 2024.
- It is predicted that by 2025, 45% of organisations will have experienced attacks on their software supply chains.
- In 2023, 39% of businesses in the UK discovered that they had been the target of cyber-attacks.

Market drivers & growth

- According to InfoSecurity, a coordinated global cyber-attack, spread through malicious email, could cause global economic damage anywhere between $85bn and $193bn.
- Regulators are training a keen eye on cyber security / data management standards:
  - Data breaches at British Airways and Marriott Hotels have led to record-breaking ICO fines of £183m and £99m respectively.
  - The Federal Trade Commission has approved a fine of roughly $550m against Facebook for mishandling users' personal information.
- Global ransomware costs are expected to exceed $42bn by the end of 2024.
- The increasing interconnectivity and interdependence of technology and business are driving the demand for companies to enhance their insurance solutions.
- As of January 2024, there were 5.35bn internet users worldwide.

Protection options

While there is no such thing as 'standard' cyber policy, set out below are typical options available in a market-leading policy.

First party cover

- Breach response costs
- Network interruption
- Data asset recovery
- Cyber extortion
- Contingent business interruption, security & system failure
- Bricking & betterment

First party risk

Potential triggers / claims scenarios

Breach response costs:

- Coverage for the direct costs to an organisation responding to a cyber event.

Cover generally includes:

- Access to breach response team, including IT forensics, crisis management and legal support.
- Notification costs.
- Call centre costs.
- Credit monitoring / ID theft identification costs.
- PR consultancy costs.

Data breach & security failures:

- A data breach is any security incident in which unauthorised parties gain access to sensitive data or confidential information, including personal data or corporate data. Security failure relates to the malicious acts of a third party.

Data asset recovery:

- The cost of external experts to recover or reconstitute lost data or software. This can be extended to include the recreation of a database which has been irreparably damaged.

- Security breach.
- Operational failures.

Typically extends to lost data due to:

- Modification.
- Deletion.
- Encryption.
- Corruption.

Contingent business interruption (CBI), security & system failure:

- A cyber CBI loss occurs when an insured suffers lost income as a result of an interruption in service performed by a specific IT service provider.

- Typically this loss will be triggered by security failure of the service provider, but in some instances can extend to system failure, for example, if a cloud service provider is temporarily unable to offer its services in the wake of a cyber-attack it has suffered.
- In some instances, the covered third parties can be extended to include wider scheduled supply chain providers.

First party risk	Potential triggers / claims scenarios
Bricking & betterment • During a cyber-attack, physical equipment may be compromised, damaged, or rendered useless due to malware. Anything from a USB drive to a laptop or a server may be damaged so badly that it can no longer function as anything other than a brick. Bricking coverage may replace those items. • If an insured needs to replace damaged software and it is no longer available to purchase, coverage can be arranged for the cost to update that software typically subject to a cap of 125% of the cost of your original software.	• Security breaches e.g. transmission and receipt of malicious code, denial of service.
Network interruption: • Indemnity for loss of income linked to the unavailability of IT systems as a result of a network disruption.	**Security failure:** the malicious acts of a third party. **Operational error:** includes accidental interruption due to a non-malicious act, or a security failure due to network interruption. **Full system failure:** any unplanned outage maybe sometimes be offered.
Cyber extortion: • The costs of IT experts to validate the threat. • The cost of external experts to assist in negotiations. • The actual monetary amount of a ransom payment.	• Threat to release personally identifiable information. • Threat to prevent access to the insured's IT systems. • Threat to introduce malicious code. • Ransomware for example, Cryptolocker, WannaCry, and NotPetya.

Third party cover

- Data privacy liability
- Network security liability
- Multimedia liability

Third party risk	Potential triggers / claims scenarios
Data privacy liability: • Liability claims arising from the unauthorised disclosure of personally identifiable information. • Liability claims arising from the unauthorised disclosure of 3rd party confidential information. • Failure to initiate a timely breach response. • Legal fees associated with defence costs. • Fines and penalties (where insurable by law). • Regulatory charges and costs of dealing with regulators as a result of a data breach.	• A rogue employee has publicised personally identifiable information. • An employee has left a laptop on a train containing files with personally identifiable information. • A cloud provider / data storage company used by the insured suffers a breach.
Network security liability: • Negligent transmission of a virus by the insured. • Denial of authorised access to third parties / customers. • The insured's participation in a distributed denial of service attack (DDOS). • The destruction of a third party's digital assets stored by the insured.	• Accidental spread of malware by the insured to a third party causing them a financial loss.
Multimedia liability: • Defence and settlement of liability claims from third parties due to the insured's content on its website. • Forms of electronic content e.g. email, intranet, newsletters etc. • Cover can be extended to content from non-electronic sources.	• Invasion of privacy. • Negligent publication. • First party risk potential triggers / claims.

Common extensions & sub-limits

Reputational harm

If as a result of a covered breach, an insured suffers damage to its reputation which results in a loss of income, cover can be extended to a loss of income as well as the increased costs of working and PR costs involved.

Social engineering / e-theft

Threat actors have developed increasingly sophisticated methods to defraud companies. In a typical case of social engineering, fraudsters pose as legitimate individuals, such as a company director or senior manager, a supplier, or a customer. They then leverage the social status or business relationships of the individual to illicit a fraudulent bank transfer from an unwitting victim.

Physical damage / bodily injury

A coverage option which may be available is physical damage as a result of a cyber event. This is either provided through a carve back or through affirmative coverage. Capacity continues to increase for this coverage option.

Loss mitigation

Coverage can be extended to include any professional fees charged by a particular third party provider, to avoid or mitigate the consequences of a breach.

Cryptojacking (service fraud)

Cyber criminals have increasingly turned to malware that mines cryptocurrency to hijack the processing power of large numbers of computers, smartphones, and other electronic devices, to generate revenue.

Service fraud coverage reimburses the insured for direct financial loss for fraudulent use of electricity and other business services.

Voluntary shutdown coverage

Affirmative cover may be available for the associated costs of willingly shutting down part of an insured's network (typically on the order of a CISO or regulator), in order to protect the network from the more damaging prospect of an expected breach.

With this added cover, businesses can protect their systems and make timely, more informed decisions.

Risk management budget

This can sometimes be provided to the insured when purchasing the policy, in the form of a return premium. The RP must be spent on relevant services that will improve the insured's security posture.

Cyber liability

Our Technology, Cyber and Media Liability team has the in-depth technical knowledge and global marketing skills to provide tailored solutions to all clients.

We understand that individual insureds and the sectors in which they operate pose a set of unique exposures. Our approach is designed to cater for, not only a variety of industry sectors, but also small firms to large corporate entities.

Expertise

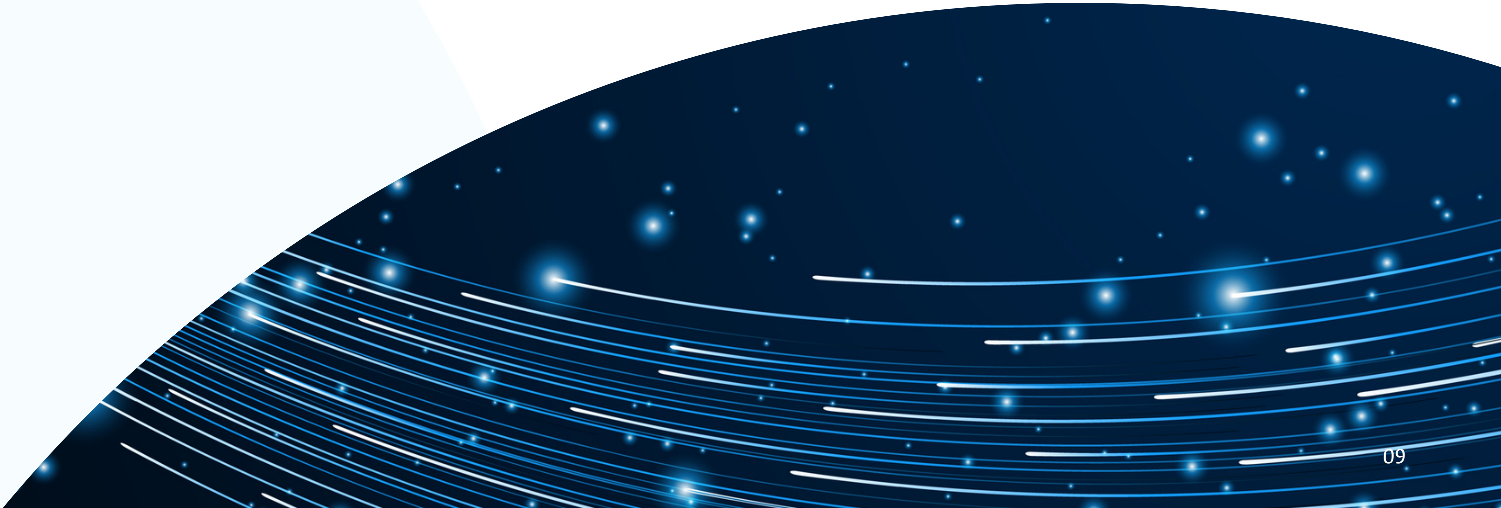
- Professional diversity; in-team solicitor and underwriter experience complement extensive broking experience to deliver best client outcomes.
- 40+ years of technical cyber placement experience.
- Experience of navigating hard market cycles.
- Direct engagement with client boards as to renewal options and recommendations.
- In-team claims specialists who form part of the client service team.

Markets

With access to over 45 carriers, our team is positioned to ensure that we are able to find the best possible solutions for our clients.

Approach

- A technical product and client service-led approach.
- Full service offering and service team continuity from first introduction, throughout placement and ongoing servicing and claims.
- Differentiating clients from others in their sector, building a positive risk profile to help increase insurer appetite.
- Structured and strategic engagement with markets to ensure an optimised insurance programme aligned with clients’ risk appetite and objectives.
- Consultative approach to cyber risk management, leveraging strategic partnerships to offer value added services, improving risk profile.



Additional information
– cyber insurance as a service

Already risk managers view their cyber insurance as more than just means to financial reimbursement.

Most policies purchased will provide not only relevant coverage, but also access to a suite of third-party breach response providers, including IT forensics, legal and PR counsel, and many more.

Now more policyholders are also utilising pre-breach services made available via certain insurance policies, to ensure they safeguard their assets and operations.

Employee training services

Can include training on phishing emails, password security, employee awareness and more.

Incident response planning

Within a tabletop exercise specialists can accurately simulate the impact of a breach, based on the most relevant threat actors, conducted with the insured's C-suite plus other relevant stakeholders.

Risk assessment services

Risk modelling and prediction can be performed quickly and add colour to a risk manager's understanding of the likely frequency and severity of a hypothetical breach.

Compliance review

With regulators across the globe bringing cyber security standards into sharper focus, and issuing a number of fines in the past two years, adhering to best practices has never been more important.

Service offerings / partnerships:

Alongside our team's technical knowledge, we have the following partnerships should our clients require them:

CyberCube

CyberCube delivers the world's leading cyber risk analytics for the insurance industry. Their cloud-based platform helps insurers to make informed risk decisions, anticipate trends before they become claims and address complex challenges. CyberCube's unique data, advanced analytics and cloud-based technology assists with insurance placement, underwriting selection and portfolio management. The team are experts in data science, security, threat intelligence, actuarial science, software engineering and insurance, all of which helps them in selecting the best sources of data to identify reliable early risk indicators.

KYND

KYND provides cyber risk management for organisations of all sizes. Their innovative and industry first technology helps businesses of any size to monitor and comprehend the cyber risks they face, act if necessary and be alerted to future risks as they arise. KYND's cyber risk products offers a simple and cost-effective solution to incorporate cyber risk management into the core of every business.

Zero Trust Security Solutions

Zero Trust Security Solutions is a cyber security firm that provides consultancy and technology solutions to help protect companies against security challenges. The Zero Trust team members' expertise and experience lie in offering their Zero Trust Architecture to collaborate with businesses to understand their threat landscapes so they can empower businesses and solve their cyber security challenges. Zero Trust work with a number of the highest ranked security software companies.

Find out more

Our cyber specialists are working with clients across the globe to create cyber insurance solutions.

Henry Warner
Managing Director – Cyber
T: +44 (0) 7940 427 492
E: henry.warner@bishopsgateinsurance.co.uk

Caroline Richardson
Director – Practice Leader – Cyber
T: +44 (0) 7787 098 467
E: caroline.richardson@bishopsgateinsurance.co.uk

Charlie Cox
Assistant Director – Senior Broker – Cyber
T: +44 (0) 7511 167 473
E: charlie.cox@bishopsgateinsurance.co.uk

Daniel Harford
Account Executive – Cyber
T: +44 20 7204 4992
E: daniel.harford@bishopsgateinsurance.co.uk

Laura Betts
Account Executive – Cyber
T: +44 (0) 742 3692 552
E: laura.betts@bishopsgateinsurance.co.uk

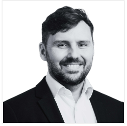
Tanjina Hussain
Account Handler – Cyber
T: +44 (0) 7721 741 581
E: tanjina.hussain@bishopsgateinsurance.co.uk

John Head
Director – Practice Leader – Cyber
T: +44 (0) 7999 047 103
E: john.head@bishopsgateinsurance.co.uk

Elle Day
Director – Practice Leader – Cyber
T: +44 (0) 7770 923 155
E: eleanor.day@bishopsgateinsurance.co.uk

Alex Cappuccio
Assistant Director – Senior Broker – Cyber
T: +44 (0) 7769 927 372
E: alex.cappuccio@bishopsgateinsurance.co.uk

Vanessa Cathie
Executive Director and Special Counsel
T: +44 (0) 7919 293 293
E: vanessa.cathie@bishopsgateinsurance.co.uk



Christopher Manning
Senior Technical Account Manager - Cyber
T: +44 20 7204 4962
E: christopher.manning@bishopsgateinsurance.co.uk

Amaia Robbins
Technical Account Manager - Cyber
T: +44 (0) 744 9971 962
E: amaia.robbins@bishopsgateinsurance.co.uk

Ardonagh
SPECIALTY

Bishopsgate is part of Ardonagh Specialty, the largest independent specialty broker in the London market. Ardonagh Specialty is owned by The Ardonagh Group, a top 20 broker globally.

Bishopsgate

Ardonagh Specialty Holdings Ltd incorporates Ardonagh Specialty Ltd (and its appointed representative Inver Reinsurance Brokers Limited), Besso Limited, Bishopsgate Insurance Brokers Ltd, Compass London Markets Ltd, Ed Broking LLP, Oxford Insurance Brokers Limited, and Piiq Risk Partners Ltd which are authorised and regulated by the Financial Conduct Authority using the trading names Price Forbes & Partners, Inver Re and Bishopsgate Insurance Brokers.

Registered office address: 2 Minster Court,
Mincing Lane, London, EC3R 7PD

140-2307