


Gallagher

Insurance | Risk Management | Consulting

CYBER AND DATA INSURANCE MARKET OVERVIEW, UPDATE AND RISK MANAGEMENT STANDARDS

GALLAGHER PUBLIC SECTOR PRACTICE

INTRODUCTION

It is clear that we are witnessing a significant reappraisal in the Cyber and Data insurance market and those funded by the public purse are feeling these changes arguably more than any other sector.

What is driving this change?

Simply put, significant increases in the frequency and severity in the claims environment, driven primarily from ransomware events.

Governments, councils, universities, schools, NHS trusts and local authorities have been the targets of these for several reasons, including highly desirable data (pandemic research), perceived inferior security controls to commercial organisations and sensitivity of institutions to damage reputations.

These claims often involve several parts of a Cyber and Data insurance policy beyond extortion, such as breach response, business interruption and data restoration.

As such the market is in a correction phase across the board, but particularly in this sector.

How is this being evidenced in subsequent purchase and procurement, and the subsequent insurance cover and protection?

The following is being witnessed across the education sector for Cyber and Data insurance:

- Significant premium increases, ranging from 50% to 300% or more
- Fewer insurers willing to offer Cyber and Data insurance coverage for education accounts. Many have pulled out completely, particularly for larger entities in urban settings requiring higher limits of indemnity
- Higher retentions/deductibles. It is not uncommon to see retentions move from £25,000 to £250,000+ in a single renewal cycle
- Sublimits and co-insurance for Cyber Extortion/Ransomware coverage from certain insurers (if limits are available at all)
- No wavering on the requirement for Ransomware Supplemental Applications
- For accounts with claims: expect to demonstrate steps taken and investments made to ensure non-recurrence
- Used by underwriters and their risk engineering teams of scanning technologies to assess remote network access vulnerabilities
- Implementation of Multifactor Authentication

How should existing policyholders or those wishing to source cover prepare?

- Start the renewal discussion and data collection process early. We suggest a minimum of six months but in reality probably longer to ensure better results
- Expect the need for great detail in the application process
- Expect (and budget for) significantly higher premiums, retentions and fewer market options. Cyber and Data insurance is experiencing a maturing as underwriters quantify and analyse losses. This comes at a time when many institutions have recognised its importance to be able to support broader Information Security Risk Management to be able to ensure operational continuity
- Examine the insurance carriers' minimum security requirements. We can then work with in-house teams in providing risk management advice to meet these security requirements:
  - Implementation of Multifactor Authentication for all users (including all remote access)
  - Properly configure Remote Desktop Protocols (RDP)
  - Deployment of advanced endpoint detection and response (EDR). These are a category of endpoint security tools, built to provide endpoint visibility, and are used to detect and respond to cyber threats and exploits
  - Ongoing employee training in InfoSec best practices
  - Phishing simulation campaigns
  - Software patch management
  - 3-2-1 data back-up strategy (3 copies; 2 local, but on different mediums; 1 offline and completely segregated from the corporate network), encrypted and tested regularly

It is worth highlighting that with the changes in the market, Cyber and Data insurance is not able to function as a protection in the absence of security measures. Instead, insurers are looking to see that it is part of a wider holistic approach to Information Security Risk Management. If a client fails to meet the security requirements outlined above for insurers, they will simply be declined from a new risk perspective or nonrenewed for existing purchasers.

MARKET COMMENTARY

Underwriters have begun to structure their requirements in line with the scope, size and profile of risks, and this falls broadly into the revenue of the organisation in question.

We have therefore broken this down between three segments as follows:

1. SME (£0-£50m turnover)
2. Mid-Market (£51m-£400m turnover)
3. Large/Macro (£400m+)

SME (£0-£50m turnover)

Minimum Insurer Requirements

Insurer Submission Requirements:

- Pen Micro SME Cyber Application (Mandatory)
- Gallagher Mid-Market UK Cyber Application (Preferred)
- Beazley Ransomware Application Form (Preferred)

Minimum Risk Requirements

- Does the insured or their outsourcer back up their data at least once a week and store data in an off-site location?
- Does the insured have antivirus and firewalls in place and are these regularly updated (at least quarterly)?
- Does the insured have remote access to desktops or servers or applications enabled?
- Do employees utilise Multifactor Authentication when accessing all desktops or servers or applications remotely?
- Can the insured recover all of their business-critical data and systems within 10 days?
- Is the insured aware of or have any grounds for suspecting that any circumstances exist which might give rise to a claim?
- Within the last five years, has the insured suffered any loss of the nature covered by this policy, or is he/she aware of any circumstance which could give rise to such a loss.

In order for an insured to be insurable, the above criteria needs to be satisfied in full. Note: MFA implementation is only required if the insured has remote access to servers or applications enabled. Obviously, the last two questions are in relation to previous claims/potential circumstances.

Note the minimum requirements above are in respect of Pen Underwriting solely. Beazley will require full completion of their ransomware form application on dependent upon the overall score will review and decide upon insurability. CFC, Aviva and NMU have slightly more flexibility from a minimum controls perspective, but given these will form open market placements, the controls and the insurability/suitability will be determined by the specific Underwriter. However, from working closely with these markets, if insureds are meeting the controls above (namely MFA) then there will be scope to obtain terms, as long as the remainder of the controls are in decent risk management condition. We can of course provide further clarity on this if required.

Limits of Indemnity (LoI) Available

£1 million-£3 million LoI

Potential Insurers

- Pen Underwriting
- Beazley Syndicate
- OSR International
- Aviva International
- NMU International
- CFC Underwriting
- Travellers

Mid-Market (£51m-£400m turnover)

Minimum Insurer Requirements

Insurer Submission Requirements:

- Gallagher Mid-Market UK Cyber Application (Mandatory)
- Beazley Ransomware Application Form (Mandatory)
- AIG Ransomware Supplemental (Preferred)

Minimum Risk Requirements

- Does the insured or their outsourcer back up their data at least once a week and store data in an off-site location?
- Does the insured have antivirus and firewalls in place and are these regularly updated (at least quarterly)?
- Does the insured have remote access to desktops or servers or applications enabled?
- Do employees utilise Multifactor Authentication (MFA) when accessing all desktops or servers or applications remotely?
- Can the insured recover all of their business-critical data and systems within 10 days?
- Filter/Scanning of emails for malicious attachments
- SPF
- Mandatory IS training
- EDR
- If RDP enabled, MFA on remote access, admin and privilege, critical info, personal devices, all applications
- Process in place for patching, three months or less
- End of support software segregated from network
- Cold storage that is completely isolated from the network
- Recovery of all critical data and systems no longer than 10 days

For any insured with revenue in excess of GBP £50 million or alternatively making a request for higher limits of indemnity (3 million+), we need to ensure the above is in place as an absolute minimum. Additional questions on the ransomware and Gallagher forms will be reviewed by Underwriters and can have a material effect on terms, but Pen Underwriting have re-confirmed if the above criteria is met then we can proceed with procuring the insurance.

Limits of Indemnity (LoI) Available

£1 million-£3 million LoI. Potentially £5 million LoI for risks with acceptable risk controls.

Potential Insurers

Markets for mid-market:

- Pen Underwriting
- Beazley Syndicate
- OSR International
- Aviva International
- NMU International
- Tarian Cyber Consortium
- CFC Underwriting
- Travellers
- Emerging Risks

This jump up in revenue/exposure will mean a number of markets listed above may be unable to quote. For example: Aviva, NMU, OSR and Tarian have maximum revenue thresholds ranging from 100 million to 250 million, so any risk in excess of this won't be eligible for a quotation through those particular insurers.

Large/Macro (Revenue: £400m and above)

Minimum Insurer Requirements

Insurer Submission Requirements:

- Gallagher Macro UK Cyber Application (Mandatory)
- Beazley Ransomware Application Form (Mandatory)
- AIG Ransomware Supplemental (Preferred)
- Additional Systemic Risk Applications (Solarwinds, log4J exposures)—Brit application form attached

Minimum Risk Requirements

- Endpoint detection and response (EDR) solution
- Operational technology covered where possible
- Multifactor Authentication with a challenge-response scheme (SMS, App, Token, etc.) for remote access
- Local administrators disabled
- Unique system administrators credentials
- Separation of admin accounts for workstations, servers, domain controllers. MFA for privileged accounts
- Privileged access is logged
- PAM solution with credential rotation and vaulting
- Vendor access is restricted in scope and is monitored
- Monthly patching and emergency patch process (<72 hours)
- Monthly vulnerability scans
- Quarterly patching of OT
- Legacy systems are protected with compensating controls
- Segmentation of networks by locations and according to "defence in depth" principle (office network, applications, databases) with governance around firewall rule changes
- Stringent IT/OT segmentation
- Host firewall rules on each endpoint
- Advanced technology for scanning and filtering of web-traffic and email-traffic (sandboxing, protective DNS, etc.)
- Sender policy framework and DKIM/DMARC are enforced
- Intrusion detection/prevention enabled and feeding to SIEM
- Web application firewalls for everything externally facing
- Training and awareness programme, phishing tests, campaigns
- Mandatory participation
- Targeted Awareness Training for administrators, finance
- Continuous 24/7 IT monitoring function
- SIEM solution and monitoring of SIEM alerts 24/7
- DLP in place and alerts fed to SIEM
- Regular testing of detective capability
- Incident response plan (IRP) and organization
- Quarterly IR exercises, including ransomware scenario
- Inclusion of third-party service providers in the IRP
- Back-up process, including offline and off-site back-upping (application and database servers, workplaces, and OT). Offline and off-site can be tapes, but can also be cloud back-up or isolated back-up host
- Encryption of back-ups
- Semi-annual testing of back-up recovery procedures for all data with high criticality. Annual full system recovery tests for key critical systems
- BCP with IT emergency scenarios defined and tested annually

Limits of Indemnity (LoI) Available

£1 million- £5 million LoI. Potentially higher for risks with acceptable risk controls.

Potential Insurers

- Pen Underwriting
- Beazley Syndicate
- CFC Underwriting
- Brit Syndicate
- Ki Syndicate
- Tarian Cyber Consortium
- Emerging Risks
- Travellers

The Macro public sector market place is one that has come under increased scrutiny due to the performance of insured's in this sector. This is both from a claims and general risk management perspective, therefore we have been told in no uncertain terms that controls have to be perfect across the board in order to be deemed insurable for Cyber Liability coverage. Obviously, the requirements listed above may change slightly when considering a 400 million revenue entity as opposed to a 1 billion+ revenue entity, but we would advise in the first instance that the above controls are worked towards and tracked against.

Gallagher Cyber Assist and Risk Consulting

Gallagher's Cyber Assist and Cyber Risk Consultancy division can assist education institutions in better understanding their current preparedness around Information Security Risk Management.

In the same way that a property survey can help detail for underwriters the key aspects of the risk and identify the potential for improvements, the cyber risk consultants can do the same.

There are a range of tools available to help which are detailed in the attached GCA Services brochure. These will depend on each institution's profile and maturity, and the insurance cover they are seeking, and your Gallagher Client Director will be able to facilitate a discussion around this accordingly.

Would you like to talk?

To find out more, please contact your usual Gallagher representative.

Paul Latham
Client Development Executive
Public Sector & Education
M: +44 (0)78 8771 7624
E: Paul_Latham@ajg.com

James Wall
Cyber & Technology
Account Executive/Broker
T: +44 (0)207 234 4269
M: +44 (0)7506 721 853
E: James_Wall@ajg.com

Archie Ghinn
Cyber & Technology
Account Executive
M: +44 (0)7729 441 987
E: Archie_Ghinn@ajg.com

Arthur J. Gallagher Insurance Brokers Limited is authorised and regulated by the Financial Conduct Authority.
Registered Office: Spectrum Building, 7th Floor, 55 Blythswood Street, Glasgow, G2 7AT.
Registered in Scotland. Company Number: SC108909. FP424-2022 Exp. 16.03.2023.

Gallagher

Insurance | Risk Management | Consulting