Gallagher

Insurance | Risk Management | Consulting

HIGHER EDUCATION — INFORMATION SECURITY AND DATA PROTECTION

INTRODUCTION

It is clear to any business, institution, organisation or individual that we have been living through a significant change in the way the world operates, interacts and engages with each other.

Online activity is now prevalent and perhaps pre-eminent in our work, family and leisure time.

This revolution has brought data front and centre. The consensus is now that data is the 'oil of the 21st century' and amongst the largest, most critical companies, in the world are those that trade on, control and manage our data.

The pandemic has heightened the fact that for education institutions, information security and technology platforms now play a critical role in delivering services as well as control of estate and infrastructure.

Further, the ground-breaking research that universities are involved in is at threat from those who would seek to gain, benefit or potentially interrupt this.

If the central tenets of insurance and risk management are around protecting and financially supporting the key sources of revenue and assets that are controlled it is inevitable that questions will be asked as to how we insure and protect our on-line activity and our data.

Legislation is now in place which recognises this and any prudent insurance and risk manager or anyone involved in the purchase or administration of insurance should be asking about what support is available.

This Technical Bulletin examines how the insurance market has developed and evolved, and the backdrop against which this has happened. It explores the key risk questions that Higher Education Institutions (HEIs) need to be posing to themselves. Most crucially it looks at the future role of risk management which, as with any class of insurance, now has a critical role to play in how cover is purchased and structured.

Our position as brokers and consultants is that on a co-ordinated and consistent basis the risks internally should be managed as best possible and from here a sensible discussion is then had on the residual risk, and whether and how this can be transferred via an insurance contract.

.

Phil Webster
Executive Director, Education

OUR VIEW OF THE CURRENT MARKET

Archie Ghinn and James Wall, Cyber Technology Practice, Gallagher

It is clear that we are witnessing a significant reappraisal in the cyber and data insurance market and no sector is feeling these changes more than education.

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:

- Premium increases.
- Fewer insurers willing to offer cyber and data insurance coverage for education accounts. Many have pulled out completely, particularly for city, larger entities requiring higher limits of indemnity.
- Higher retentions/deductibles. It is not uncommon to see retentions move from £25K to £250K+ in a single renewal cycle.
- Sub-limits 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.
- Use by underwriters and their risk engineering teams of scanning technologies used 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 help ensure optimal 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 (MFA) 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 may simply be declined from a new risk perspective or non-renewed for existing purchasers.

JISC AND THE ROLE OF CYBER SECURITY IN YOUR HEI

16 questions you need to ask to assess your cyber security posture

1. Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?
2. Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leaves our organisation?
3. Do we review user accounts and systems for unnecessary privileges on a regular basis?
4. Do we enforce multifactor authentication for all systems and users?
5. Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?
6. How long will it take us to recover critical business functions, assuming a loss of all infrastructure? What's the business impact of a loss of all digital infrastructure? How will we lead and co-ordinate business recovery in this scenario?
7. Can the organisation tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our organisation?
8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?
9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?
10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?
11. How would our organisation identify an attacker's presence on the network?
12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?
13. Are all staff aware of and participate in effective cyber risk management processes?
14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training advice and guidance?
15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?
16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?

Jisc can help you strengthen your position—get in touch to find out how we can support your institution: **securityservices@jisc.ac.uk**

THE ROLE OF RISK MANAGEMENT

Johnty Mongan, Managing Director, Gallagher Cyber Assist

In our experience, it's becoming increasingly difficult for HEIs to obtain insurance cover for their data/cyber risks. Exposures have grown significantly following the move to agile working and increased threats particularly from ransomware attacks and this leads to increasing claims costs and pressure on insurance premiums.

As a consequence Insurers are requiring more detailed information about how cyber and data protection risks are managed, and their proposal forms can sometimes be complex.

Due to the high risk of ransom claims and their resultant costs, insurers want to see high standards of risk control. Many insurers are now insisting on risk reduction features such as multifactor authentication, training and segmentation before they quote.

Obtaining terms is no longer as easy. Gallagher Cyber Assist recommends a three-stage process as follows:

1. Audit and vulnerability scanning

Undertake a comprehensive audit of your IT infrastructure to identify weaknesses and vulnerabilities. We recommend using the internationally recognised Common Vulnerability Scoring System (CVSS) to capture the principal characteristics of a vulnerability.

The ultimate aim is a comprehensive audit that will identify what is susceptible and the remediation required.

The results should be included in your Market Prospectus (See Point 3).

2. Risk improvement plan

Once your vulnerabilities are detailed and understood, we recommend developing a plan to improve your cyber strategy, defences and resilience. This could include elements such as:

- Staff training or awareness campaigns to reduce people risk—many breaches result from simple errors.
- Design of processes, procedures and board-level reporting templates to ensure visibility and control.
- Gain accreditation to information security standards such as Cyber Essentials, Cyber Essentials Plus and IASME Governance.

This plan should also form part of the Market Prospectus (see point 3) regarding communication to insurers on what you have implemented.

3. Create a bespoke Market Prospectus for your risk

It's imperative that the insurers fully understand the risks they're being asked to insure. If they don't, it's easy for them to say "no". A Market Prospectus will help you provide all the information your insurers' need, in a clear format that underwriters will want to read. We recommend drawing together all relevant personnel in your organisation—IT, legal, data protection, financial, HR—to obtain all the information insurers need to provide a quote.

The aim is to produce a comprehensive prospectus to support your application for insurance. This will:

- describe your risk profile in detail;
- communicate the important controls you have in place to protect your organisation; and
- give your appointed broking team the detailed information they need to 'present' your risk to insurers.

The end goals here are to:

- help your university obtain the insurance protection you need at an acceptable cost;
- help your university fully understand their data/cyber risks and the effectiveness of existing controls; and
- identify any changes your university needs to make to improve your resilience.

To find out more, please contact our Cyber Risk Management team:

CyberRM@AJG.com

Would you like to talk?

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

Phil Webster
Executive Director, Education

M: +44 (0)7717 802 518
E: Phil_Webster@ajg.com