



Cyber Risk Management Global Practice

2022



Gallagher

Insurance | Risk Management | Consulting



Welcome to Gallagher's Cyber Risk Management Practice

We live and work in a world where cybercrime can no longer be regarded as something that happens to other people, other businesses, and other organisations. The reality is that no person or business is immune from a cyber-attack or data breach—whether due to criminal intent or employee error.

There has been a notable rise in cyber-related claims in recent years, driven by the growth of the cyber insurance market but also by the rise in incidents such as data breaches, distributed denial of service attacks, phishing campaigns, and increasingly, ransomware events which are becoming the dominant cause of losses.

While cyber insurance can offer some protection from the financial consequences of a cyber incident, it is just one element of an effective Cyber Risk Management programme. Taking a proactive approach to cyber risk is becoming increasingly important for organisations of all sizes, not only to protect themselves and their clients, but also to secure specialist cyber cover in an increasingly challenging insurance market.

Johnty Mongan

HEAD OF CYBER RISK MANAGEMENT

Underwriters typically want to see evidence of your Cyber Risk Management protocols before agreeing to offer insurance. This is where partnering with a specialist in cyber risk can help you secure cover, while at the same time taking the necessary steps to strengthen your organisation's digital armour. One of the services we offer, Gallagher Cyber Assist, is designed to help you achieve both—enhanced cybersecurity and adequate cover. You can watch a short video about the service [here](#), and also find out more on page 21.

This brochure details all the services our Cyber Risk Management practice offers to enable you to improve your cyber strategy, defences and ability to recover from a cyber incident.

We will work alongside you as your long-term Cyber Risk Management partner—helping you protect your organisation against one of the most significant risks facing businesses today.



Contents

Global capabilities	4
Strategies for your business size	5
Case studies	6-7
Our cyber services	
Gallagher Cyber Defence Centre	9
Gallagher Cyber Assist	10
Cyber Essentials Implementation and Accreditation	11
IASME Implementation and Accreditation	11
ISO 27001—Readiness and Implementation	12
Penetration Testing	12
Cybersecurity Awareness Training	14
Vulnerability Scanning	14
Gallagher GDPR Audits	15
Virtual Data Protection Consultant as a Service	15
Phishing Simulation	16
Maturity Assessment—DEFCON 6	17
Incident Response Planning	19
Cyber business continuity planning	20
Cyber Risk Management webinars	21
Insurance as the bottom line	22
Cyber Risk Management practice combined qualifications	23

Global capabilities

Cybersecurity is borderless and traverses all industries, sectors and regions. Each territory has local laws which we are capable of consulting in. We have clients all across the world utilising our expertise. We have a dedicated team to support our clients in the USA, where HIPAA controls are required and supporting all non-EEA countries with their requirements to comply with data processing of any EU citizen.

To deliver our security assessments overseas, we deploy our own technology to allow us to virtually be on-site. This saves time and cost for our clients and is unique to our offering. Our clients can benefit from the borderless service we offer, and take advantage of our breadth and depth of knowledge. Any organisation has a place in our family of clients, and geography places no boundaries for what we can accomplish.





Strategies for your business size

We offer a range of strategies for every size of business and every budget, from multi-national corporations to SMEs. Below is an idea of the services we offer for each type of business, while recognising that every organisation is unique—we will work with you to determine the most appropriate services for your cyber risk. We can offer our services on a retained basis as your ongoing Cyber Risk Management partner.

Corporate

For larger businesses, we can offer a suite of services, including the design and implementation of a bespoke cyber business continuity plan which stands as the blueprint document in the event of a cyber-attack.

Mid-corporate

For mid-sized corporate businesses, we offer a cybersecurity awareness course, which helps your business identify and avoid the most common pitfalls small businesses face, as well as Cyber Essentials compliance and accreditation services. For organisations looking for a more comprehensive information security standard, we offer IASME compliance and accreditation services.

SMEs

For smaller businesses, we offer the same cybersecurity awareness course as we do for mid-sized corporate businesses, and we supply Cyber Essentials compliance and accreditation services.

Care home client held to ransom

When a Gallagher client in the care home sector suffered a serious ransomware attack, Gallagher's Cyber Risk Management practice team initiated a swift breach response service to get the business back up and running quickly.

In June 2020, a Gallagher care home client suffered a serious ransomware attack which encrypted all assets and prevented them from being able to fully trade. We offered our breach support response service, and a team was immediately put together. The breach was managed over a period of eight weeks, with daily contact with the client, and a detailed investigation on the date of the attack, how access was gained to the client's systems, the type of ransomware attack and its origin.

The client's systems and data were restored in phases, new security hardware and software installed, passwords were reset for all users and Multi-Factor Authentication introduced. Approximately five weeks post-attack, the business was back up and running, without the need to pay the ransom demand. Cybersecurity awareness training was provided to give them the knowledge and confidence to recognise and combat further emerging cyber threats, and we liaised with insurers to secure cyber cover, outlining the actions the client had taken to bolster their cyber defences.



Tackling cyber risk behind the scenes

Gallagher's Cyber Risk Management practice reviewed the cybersecurity of a major retailer, providing detailed information on their areas of exposure, recommendations for action, and advice on engaging with the insurance market with regard to cyber cover.

Starting with a 30-minute consultation, the team began by including an open source intelligence exercise to highlight vulnerabilities in the client's IT systems. On carrying out a thorough review, we provided the following services; Cyber Essentials, Cyber Essentials Plus and IASME Governance Standards, working with heads of HR and IT and the Data Protection Officer.

We undertook vulnerability scans for both internal and external facing IP addresses to identify any known vulnerabilities, and a penetration test was also carried out by an 'ethical hacker' with the client's permission to test their network and systems in order to identify potential weaknesses that could be exploited by cybercriminals.

The final report included a comprehensive threat analysis and cyber risk review, with our recommendations and actions for the client in order to ensure they meet the relevant governance standards. The information we provided also enabled informed conversations with insurers to gauge their initial thoughts on the provision of a cyber insurance policy.





Cyber Risk Management Practice:
Our Cyber Services

Our Cyber Services

Gallagher Cyber Defence Centre

Gallagher Cyber Defence Centre is ongoing package of support, available as an annual service to Gallagher policyholders in any business sector. It gives members access to cyber risk specialists and offensive security technology, and includes the following services.

Vulnerability scanning—We will monitor your external boundaries and provide you updates on known vulnerabilities every 14 days.

Threat intelligence webinars—Using our extensive intelligence on the latest threats and methods of attack, we will provide real-time updates on where your organisation needs to be focusing its cyber defence efforts.

Secure humans—Cybersecurity training webinars designed for your employees at all levels of understanding.

Virtual cybersecurity officer—Monthly virtual summit hosted by key specialists in our team, signposting the latest insights on how to secure your network.

Gallagher Cyber Risk Matters newsletter—Regular email updates on the latest cyber thinking so that you can stay informed.

Dark web scanning—We will monitor the dark web for mentions or statements about you, or your company, and informing you if your name/domain or company is a victim of criminal activity.

Cyber Essentials—Access to lower prices on Cyber Essentials and IASME accreditation.

Community intelligence—You will be invited to monthly discussions, where we will be bringing forward thought leadership and solutions for network configuration, technology optimisation, risk management and risk transfer.

Other security services—Services such as penetration testing, phishing simulations, ISO 27001, incident response planning, maturity assessments and more, are all available to you when you become part of our community.

This service is charged at a fee of £1,495 plus VAT per organisation per year.



Our Cyber Services

Gallagher Cyber Assist

This service is charged at a fee of £2,495 plus VAT, and includes:

- Comprehensive cyber insurance market prospectus.
- Audit and vulnerability scanning, and report.
- Risk improvement plan, including support to achieve Cyber Essentials.



Gallagher Cyber Assist Lite

This service is charged at a fee of £250 plus VAT, and includes:

- A 'lighter' version of Gallagher Cyber Assist, to suit smaller organisations and budgets.
- Two hours' support time to assist on calls helping you understand what insurers require and how it would integrate with existing systems.
- Bespoke guidance on how to implement controls which insurers want to see.
- Essential support to navigate technical conversations with insurers.



Our Cyber Services

Cyber Essentials Implementation and Accreditation



- Government-backed scheme created by the National Cyber Security Centre.
- Protects companies against a wide variety of common cyber threats. The standard identifies issues in configurations and processes.
- Gallagher's process includes checking over 60 controls, producing a gap analysis, recommending implementations and finally accrediting your business.

IASME Implementation and Accreditation



- The IASME Governance Standard is a cybersecurity standard, which includes a Cyber Essentials assessment and a GDPR compliance assessment.
- Created as a more cost and time effective alternative to ISO 27001 for smaller businesses with different requirements.
- A comprehensive programme, requiring compliance to over 150 controls. Holders of this standard demonstrate excellent cybersecurity and data governance practices.



Our Cyber Services

ISO 27001—Readiness and Implementation

- ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS), specific to your organisation.
- ISMSs are built on the CIA triad; Confidentiality, integrity and availability.
- An 'all bases covered' approach, this project is an internationally recognised standard, and requires an incredible level of detail. ISO 27001 is the pinnacle of ensuring information security within an organisation.

Penetration Testing

- A penetration test is an ethical hack of your network, to identify vulnerabilities and ultimately strengthen the security of your network.
- The penetration tester will test internally and externally. External testing involves evaluating externally visible infrastructure, with the aim of gaining access. Internal testing mimics attacks behind a firewall, identifying how much damage could be done in the event of a breach.



“

The cybersecurity industry has changed considerably in the last few years. Services and hardware are now being moved off-site and into cloud-based solutions, meaning that security testing has had to adapt to a more holistic approach.

While porting services to the cloud removes a lot of security maintenance concerns, such as patching and password policies, it has pushed attackers to target the most vulnerable element of a network—the human component—through both social engineering and targeted attacks, to access internal services and systems.

Penetration testing simulates an attacker’s mindset when approaching a target. It now involves a phased approach to testing all the separate components of the network infrastructure and determining how each component can directly or indirectly pose problems for each other.

Before working as penetration tester in the commercial sector, I carried out cyber and digital investigations in the police force, and later covert tracking and hacking of digital devices and computer-based forensics. The landscape always was and always will be evolving, but penetration testing as a service will still follow the same testing methodology to look for vulnerabilities in authentication and active services—with the same end goal to help clients close these vulnerability gaps and strengthen their defences.”

Jay Lucas

Cyber Risk Technical Manager/Penetration Tester, Gallagher Cyber Risk Management Practice



Our Cyber Services

Cybersecurity Awareness Training

- Hour-long sessions delivered remotely to your staff members, identifying varying elements of cybercrime, and how to stay vigilant against them.
- Sessions cover a host of topics from the illegal sale of passports and guns on the dark web to ransomware and spyware.
- New modules to identify the dangers of working from home and how you can defend against common attacks.

Vulnerability Scanning

- A continual service offered by the Cyber Risk Management team, with one run each month.
- Ongoing vulnerability scanning against your publicly facing assets, identifying potential vulnerabilities and exploits.
- A comprehensive report is supplied identifying which ports are susceptible to attack, and the steps of remediation required.



Our Cyber Services

Gallagher GDPR Audits

- Gallagher GDPR compliance assessment is a turnkey solution for those organisations looking to assure compliance.
- Within this audit, Gallagher will identify those practices and processes that fall outside of compliance with the General Data Protection Regulation.
- Gallagher will produce a comprehensive risk-based gap analysis that outlines which areas of noncompliance require immediate support positioned against those actions that need to be addressed after all critical tasks are complete.
- Following the audit, Gallagher will produce its bespoke GDPR compliance report. This report will outline those actions required to achieve regulatory compliance.

Virtual Data Protection Consultant as a Service

- Gallagher DPC as a service will inform and advise you and your employees of your obligations to comply with the GDPR and other data protection laws.
- Gallagher will monitor compliance alongside your in-house DPO, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits.
- We advise, monitor and conduct data protection impact assessments.

Our Cyber Services

Phishing Simulation

Phishing poses a real threat to your organisation and your employees. A phishing email will try to obtain sensitive information from your employees such as login or bank account details and use this information to commit fraud, extortion and/or identity theft.

We recommend a multi-layered approach to phishing, in addition to cybersecurity awareness training, we offer a phishing simulation service that tests your employees' ability to identify and report phishing emails.

Responding to emails and clicking on links is a huge part of the modern workplace and spotting phishing emails is hard and spear phishing emails are even harder to detect.

Using phishing simulations will ensure that this subject is at the forefront of your employees' minds and furthermore enable your organisation to assess just how well your employees' are helping to protect your business.

The phishing simulation itself comprises an email campaign, undertaken over a period of three months, where users will be targeted and encouraged to click on links or open attachments.

Following each simulation exercise, we will provide you with a short report detailing what percentage of your workforce actually are cybersecurity aware and what percentage are vulnerable following a social engineering attack. The results will provide you with the data you need to determine whether any further training in this area may be required for your employees.

- 1 Target Users
- 2 Deliver Simulation
- 3 Analysis and Reporting
- 4 Awareness and Training

These simulations are aimed at changing the behaviour of your employees' so that they can recognise, avoid and report potential threats that could compromise the critical business data and systems of your organisation.

Our Cyber Services

Maturity Assessment—DEFCON 6

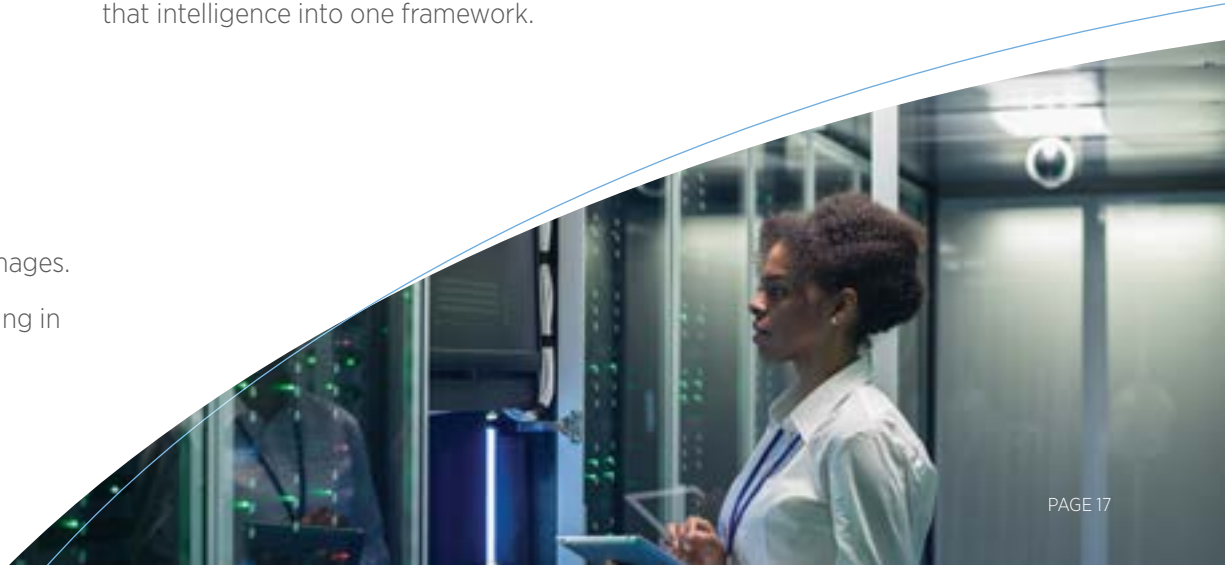
Technology is continually changing and therefore what is good today may not be good tomorrow. Gallagher has developed a maturity assessment that combines the latest threat controls, whilst consolidating the critical controls from the world's best security standards. Our DEFCON 6 audit allows an organisation to benchmark itself against a 'best-in-class' maturity standard, and put itself on an improvement roadmap over the next three years. Gallagher focuses on understanding the controls in place to mitigate the following vulnerabilities.

Ransomware—local or enterprise-wide ransomware resulting in significant BI revenue loss.

- **Data Espionage**—extortion not to expose what is known to a malicious actor.
- **Data Exfiltration/Leak**—large-scale privacy claims/class actions.
- **Malware**—data destruction/data manipulation resulting in long-term business interruption.
- **Zero-Day Exploits**—unknown attacks leading to the loss of critical intellectual property.
- **Cybercrime (Payment Fraud)**—the payment of unrecoverable funds to a malicious account.
- **Multimedia Liabilities**—hack/defacement of any public site resulting in damages.
- **Reputational Damages**—the loss of revenue due to any of the above resulting in long-term revenue decline.

- **Hardware Destruction**—the permanent damage to a legacy system that cannot be recovered due to its inherent legacy issues.
- **Social Engineering**—the exploitation of a weak workforce leading to uncontrollable accidents/breaches/leakage of sensitive information.
- **Insider Threats**—damages through loss of IP/customer relationships or reputational harm due to malicious individuals seeking revenge or closure on a grievance.

A localised vulnerability is a weakness isolated to one part of the network/organisation that cannot contribute to the wider destruction of its neighbouring systems. An enterprise-wide vulnerability is a weakness that when exploited could contribute to the mass destruction of more than one neighbouring system, creating long-term irreparable damage. DEFCON 6 is a multi-tier approach to identify both vulnerabilities. It takes the best controls from industry best practices and compiles that intelligence into one framework.



“

We are seeing the landscape shift every day in response to new threats, demands placed on clients by cyber and other insurance requirements and their own increasingly high self-governed standards. Organisations want to know exactly where they sit from an information and cybersecurity stance, and what needs improving most urgently—but they also have businesses to run, and time is often the most scarce resource.

We pioneered DEFCON 6 in the Cyber Risk Management practice team to provide a comprehensive information and cybersecurity review across all aspects of a client’s digital estate. This isn’t just a conversation, it’s a technical and behaviour-based review of how a firm operates, highlighting what is done well and what needs remediation. All put together in a readable format. We don’t adhere to the traditional consultancy model either, no wishy-washy language. We’re here to give our clients pertinent insights into their security.

In the next five years, I can foresee state-backed actors conducting more sophisticated attacks, with TTPs (tactics, techniques and procedures) filtering down inevitably to organised crime and script kiddies (unskilled hackers). This will, in time, lead to more issues from a risk management and risk transfer perspective, moving the bar for cover even higher. Couple that with a lack of cyber talent available worldwide currently, and the outlook appears bleak—but it’s not all bad! Investment and innovation to keep everyone safe are in constant battle with malicious hackers.

Individuals will get savvier and therefore so will businesses, but it’s good to have a team of cyber specialists on your side, and that’s why we are here. ”

John Clarke

Cyber Risk Consultant, Gallagher Cyber Risk Management Practice



Our Cyber Services

Incident Response Planning

Failing to prepare is often an ominous sign that an organisation is preparing to fail. Should the worst happen, it's essential that there is a set of processes and instructions in place that allow management to respond as quickly and efficiently as possible.


Gallagher's Cyber Risk Management practice can review and create incident response processes for a wide range of potential incidents, including malware infection, phishing emails successfully exploiting a vulnerable target and many more. From simple checklists to detailed playbooks, we can create bespoke solutions based on your previous experiences and what we think you're most likely to face in the future.

There is a distinction between both incident management and incident recovery. Incident management sits within and across any response process, ensuring all stages are handled, including communications, media handling, escalations and any reporting issues. Incident response focuses on triage, in-depth analysis, technical recovery actions and more.

Our development process is centred around both the best practices discussed within the National Institute of Standards and Technology (NIST) Special Publication 800-61, and the tactics, techniques and procedures of adversaries identified by the MITRE ATT&CK® framework. We identify the most pertinent controls applicable to your organisation and industry sector, and create a start to finish solution that prepares your organisation.

We run regular incident response clinics by webinar to help you plan and prepare for cyber-attacks, and improve your ability to respond and recover.



[Click here to find out more, and book a place.](#) 

Cyber business continuity planning

Our cyber business continuity planning helps your business to consider how you would react and respond to a cyber-attack. We use a three-phase approach to achieve this.



Threat Identification

We will assess the intent and capability of various threats and how likely they are to specifically target your key systems. For example, while the likelihood of a hacker using ransomware to target your business on an organisation-wide level is high, hackers are unlikely to specifically target their malware against the key systems.



Threat Assessment

The threat assessment provides an 'at a glance' assessment of priority threats. This threat map will be used in conjunction with protective measures advised by us to help secure your day-to-day operations.



Business Continuity Planning

The business continuity plan takes both the threat register and threat assessment to create a detailed and granular approach to control your company's risks. The measures Gallagher recommends are grouped into 'programmes' to reduce the risks identified.

Gallagher's cyber risk business continuity planning programme is designed to be simple and easy to understand as we want to provide your business with a clear vision of what threats could be a target, how these might manifest into specific risks to its operations, and what mitigation strategies need to be put in place now to improve your organisation's resilience to identified threats.



Cyber Risk Management webinars

The State-of-the-Nation webinar series

Throughout 2022, we are hosting a series of cyber webinars to keep you updated of the many cyber threats that may face your business as you continue to serve a remote workforce, highlighting the multitude of Cyber Risk Management solutions available to your organisation.

What you will get from this webinar series:

- Relevant information to better protect your business.
- Build your own understanding of cybersecurity from a technical standpoint.
- A look inside a hacker's toolbox. Know the tools being used and deepen your understanding of the threats.

Our panel throughout the year

Johnty Mongan, Head of Cyber Risk Management

Jay Lucas, Cyber Risk Technical Manager

Georgia Price-Hunt, Cyber Risk Consultant

John Clarke, Cyber Risk Consultant

Each webinar will be recorded and available to watch on demand. Register here for the series.



You can keep up to date with all the latest cyber webinars from Gallagher here.



Insurance as the bottom line

As cyber risk continues to evolve, and cybercriminals become more sophisticated, protecting your organisation is more important than ever. While you can't prevent every single cyber-attack from happening, you can insure against the potential impact to your business.

Cyber risk exposures have grown significantly following the move to agile working, and claims cost are increasing. These factors have contributed to the cyber insurance market experiencing hard market conditions, and this is likely to continue given the increasing risk organisations are facing in the current climate.

Most insurers who underwrite cyber insurance are now requesting that businesses have Multi-Factor Authentication (MFA) for all remote access of their systems. At Gallagher, we are seeing an increase in the number of businesses that are being refused cyber insurance cover due to a lack of MFA, leaving them exposed to significant losses.

We can help you secure cover

One of our key services is Gallagher Cyber Assist, which is designed to help you identify and improve areas of vulnerability in your systems, placing your organisation in a more favourable light to insurers. Our cyber specialists and ethical hackers will liaise with your IT team, to obtain all the technical information insurers need to provide a quote.

Once we have undertaken a survey of the cyber security controls for your organisation, you will have a tailored solution that can help to mitigate your cyber risks including breaches, malicious attacks, fraud, social engineering, human error and service provider failure. We can also assist you with developing Cyber Risk Management procedures, and following a breach, we can help you to get back on your feet, with our recommendations for breach response teams, law firms and forensic IT consultants.

We will never offer you off-the-shelf cyber policies. Our specialist team can design a cyber protection programme that is carefully tailored to your industry and even your particular business—helping you face the future with confidence.



Cyber Risk Management practice combined qualifications



BCS Level 4 Award in Network and Digital Communications



BCS Level 4 Award in Risk Assessment



BCS Level 4 Certificate in Cybersecurity



BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards



BTEC Level 3 Infrastructure Technician



CEH (Certified Ethical Hacker)



CRT



Cyber Essentials Plus Auditor



GDPR Foundation & Practitioner



ISO 27001 Implementation Lead



MCIIS (Member Chartered Institute of Information Security)



OSCP (Offensive Security Certified Professional)



OSWP (Offensive Security Wireless Professional)

About Gallagher

Founded by Arthur J. Gallagher in Chicago in 1927, Gallagher has grown to become one of the largest insurance brokerage, risk management and human capital consultant companies in the world. With significant reach internationally, the group employs over 39,000 people and its global network provides services in 150+ countries.

WE HELP CLIENTS FACE THEIR FUTURE WITH CONFIDENCE

OVER 39,000 EMPLOYEES WORLDWIDE	MORE THAN 90+ YEARS IN THE MARKET	SERVICING CLIENTS IN 150+ COUNTRIES WORLDWIDE
--	--	--

GALLAGHER HAS BEEN NAMED ONE OF THE WORLD'S MOST ETHICAL COMPANIES® FOR ELEVEN STRAIGHT YEARS. WE'VE BEEN COMMITTED TO DOING THE RIGHT THING FOR OVER 90 YEARS.



Client Testimonials

“

We were interested to hear more about the cybersecurity offering from Gallagher. From our first meeting, Johnty explained things in a non-IT way, demonstrated potential security issues/fixes and also where we could be from a cybersecurity perspective. He worked within our budget and over the past six months he has supported us, dealt with our IT company to get changes made and also been an excellent sounding board. We have found him to be open and honest, and the service offered has been transparent. We now feel confident and protected in our cyber systems and this is thanks to Johnty and his team.”

Dave Hands

Managing Director
LTS Global Solutions

“

Gallagher Cyber Risk Management practice conducted a penetration test for us that was beyond the normal type of test. They go to a level of detail that our outsourced IT provided said “they did not expect that quality”. For a risk that is so great to every organisation, we believe it is paramount to understand the exposures that exist within a network and that can only be identified by experts in their graft. I would recommend the Gallagher Cyber Risk Management practice team to any education establishment.”

Steven Groutage

Chief Operating Officer
Tudor Grange Academies Trust

“

An effortless, cost effective engagement which provided me with a clear view of my cyber exposure and clear action plan. Highly recommended. Many thanks for this. As I said, an outstanding piece of work from my perspective.”

David Cutts

Chief Operating Officer
Card Factory

Contact us

To find out more about any of our services,
please get in touch with:

Cyber Risk Management Practice

E: CyberRM@ajg.com

ajg.com/uk | [gallagher-uk](https://www.linkedin.com/company/gallagher-uk) | [@GallagherUK](https://twitter.com/GallagherUK)

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. FP364-2022 Exp. 07.03.2023.

© 2022 Arthur J. Gallagher & Co. | ARTUK-3570



Gallagher

Insurance | Risk Management | Consulting