BASED IN THE SOUTH EAST AND SERVING THE UK SINCE 1996

INTERSYS®.uk

IT Services and Security

FREE
PLEASE TAKE A COPY

NEWS FROM THE LEADING PROVIDER FOR THE INSURANCE SECTOR

IT AND CYBER RISK EXPERTS NOW IN CITY



IT and cyber risk specialist Intersys has opened an office at Leadenhall Market in the City of London. Founded in 1996, the company has served clients in the financial sector for nearly 30 years. This expansion, as reported in *Insurance Times*, puts Intersys right on the doorstep of clients in the insurance industries looking for cyber-resilient IT from a trusted UK provider.

During its history, Intersys has grown its client list across financial industries to include insurance, fintech and fund management, while also serving other highly regulated sectors such as life sciences and mining.

Says Intersys' Managing Director Matthew Geyman, 'This expansion places us at the heart of an industry we know well. I look forward to helping clients strengthen their cyber resilience and develop modern IT that drives growth.'



Intersys delivers comprehensive IT solutions for clients in the London Market. Its Security First MSP service provides complete outsourced IT management, combining remote and on-site support from a customer service-trained team. Meanwhile, Cyber Security as a Service offers cloud-based protection featuring threat detection, rapid, incident response and risk management delivered by advanced AI and expert security teams.

As a key player in the London Market's digital transformation, Intersys can help clients optimise and secure risk platforms, reduce costs, and achieve compliance with regulations or initiatives such as Blueprint Two. It also helps implement placing platforms, and systems for claims, industry reporting, actuarial analysis and exposure management.

Says Richard Geyman, Intersys' Technical Director, 'We can provide a fully outsourced "leave it to us" IT or security solution; or we can augment and support IT teams in leveraging new insurance-sector technologies.'

INTERSYS LTD CLIENTS 10X LESS LIKELY TO SUFFER CYBER ATTACK



IT and cyber security specialist Intersys has announced new performance metrics that demonstrate its industry-leading IT service delivery.

According to internal data, Intersys clients are **ten times less likely to suffer a cyber attack** than the national average. This is significant given the UK government's annual breaches survey, which reveals that half of UK businesses experienced a cyber breach in the last year.

This security track record is complemented by exceptional support desk data. Average **response time for tickets is 21 minutes**, compared to a 57 minutes industry average. Also, average **ticket resolution time is just 146 minutes**.

This superior performance is reflected in Intersys' client retention rates, which far exceed the national average – the company maintains a **94% retention rate** compared to the industry average of only 77%. Furthermore, Intersys' **clients remain with the company for an average of 8.6 years**, with many partnerships extending to 15, 20 and 25 years.

Says Mark Kirby, Intersys' Director of Professional Services, 'These figures reflect our commitment to service. Every provider says they're "committed to their customers", of course, but our numbers do add up. We've achieved this success through a "service over sales" culture – a focus on solutions rather than selling products.'

BIGGEST CYBER SCAM REVEALED: P2
84% OF BUSINESSES ARE AFFECTED YEARLY

SHOULD YOU HIRE AN AI OFFICER?: P3
INTERSYS' MD GIVES HIS VIEW

UNDERTAKING A CLOUD MIGRATION: P3
TRICKY, BUT MAY GIVE WAY TO SUNNY SPELLS

WHO IS INTERSYS, ANYWAY?: P4
A SMALL INTRODUCTION TO A GROWING PROVIDER



EBIX PRAISES ITS ‘TRUSTED PARTNER’ INTERSYS LTD

Ebix Europe Ltd, the leading insurance software provider to the London and global markets, has described IT and cyber risk firm Intersys as a ‘trusted partner throughout our digital transformation’.

Ebix required a comprehensive migration of platforms and servers to an Azure Cloud environment, including the transfer of various products, such as its digital placing system and exposure management platform, to Azure Cloud.

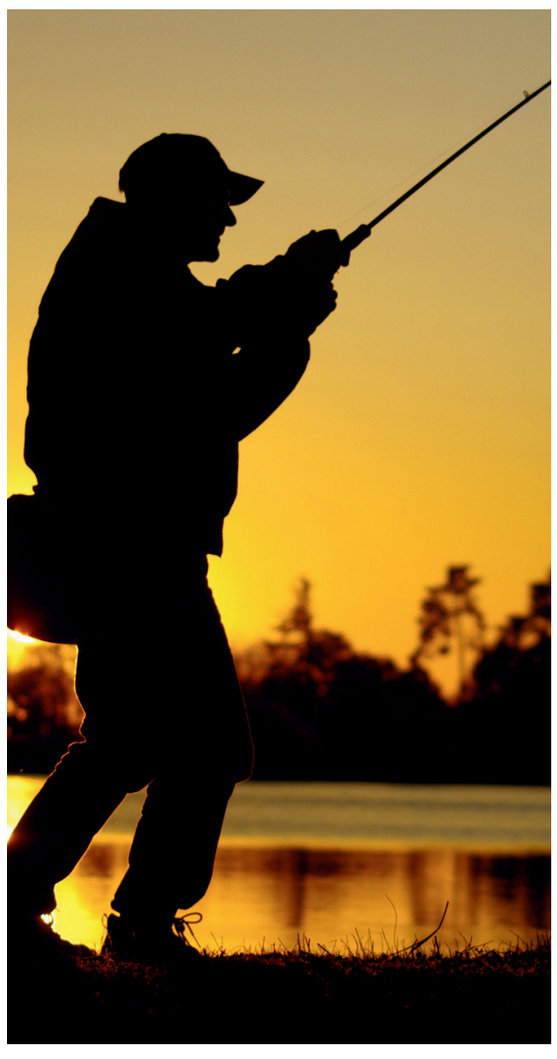
The Azure experts at Intersys are highly skilled in all aspects of virtualisation and Platform as a Service deployment environments, including SQL Managed Instance. They have also successfully executed numerous large-scale infrastructure upgrades.

Their expertise provided the necessary authority for this specialised task, which was undertaken alongside Ebix’s excellent in-house team. Intersys seamlessly managed the migration, ensuring a timely transfer that met regulations.

After the migration, the project was handed over to Intersys’ managed services team, who provide ongoing support to Ebix. Throughout the process, Intersys’ systematic approach has been key.

Said Ebix, ‘Intersys have been a trusted partner throughout our digital transformation projects. They helped drive an essential infrastructure migration to the Azure Cloud environment and enabled us to ensure that our platforms and servers were consistent, secure and aligned with best practices.’

PHISHING IS THE BIGGEST CYBER SCAM



Phishing is by far the most common cyber security breach or attack, according to the UK government’s Cyber Security Breaches Survey 2024, affecting 84% of businesses

The cost of a disruptive breach was, on average, £10,830 for medium and large businesses and £1,205 for businesses of all sizes, according to the report. However, experts in the cyber risk sector agree that costs are typically far higher when reputational damage, particularly in relation to compliance breaches, are considered.

Phishing is a type of cyber attack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing data. Businesses should also be aware of the increasing prevalence of ‘quishing’, a phishing variant using QR codes embedded in emails to lure users to malicious phishing websites.

Says Jake Ives, Intersys’ Head of Security, ‘These figures are worrying, but you can fight back. Both 24/7 network monitoring and user education are key to securing data and preventing phishing attacks.’

Visit https://intersys.co.uk/blog/ for articles on phishing, quishing and other cyber scams.



CYBER CRIME #1 RISK TO INSURERS

In a recent article for *Emerging Risk*, an online publication for corporate buyers and the (re)insurance market, Intersys MD Matthew Geyman highlighted the growing threat of cyber attacks to insurers.

An ORIC International survey, reported Matthew, ranked cyber risk as the number-one emerging risk (based on frequency) for medium firms and number four for small firms. He went on to list some of the highest-profile and devastating breaches of recent times, including the major breach to Australian health insurer Medibank which compromised sensitive and confidential health information of over 10 million individuals.

It’s no small irony, said Matthew, that insurers – who safeguard others from cyber risk – suffer devastating attacks. Neither is it surprising: insurers, he added, are ‘sitting on a goldmine of information.’ So what should they do?

Said Matthew, ‘Strengthening defences begins with adopting basic security measures like MFA, regularly updating software, and conducting frequent vulnerability assessments.’ He also referenced the need for advanced threat detection, good data storage and access management policies, encryption, and data segmentation. He concluded, ‘The insurance sector’s adoption of cyber security must go beyond protecting clients – it must protect itself.’



SHOULD YOU HIRE A CHIEF AI OFFICER?

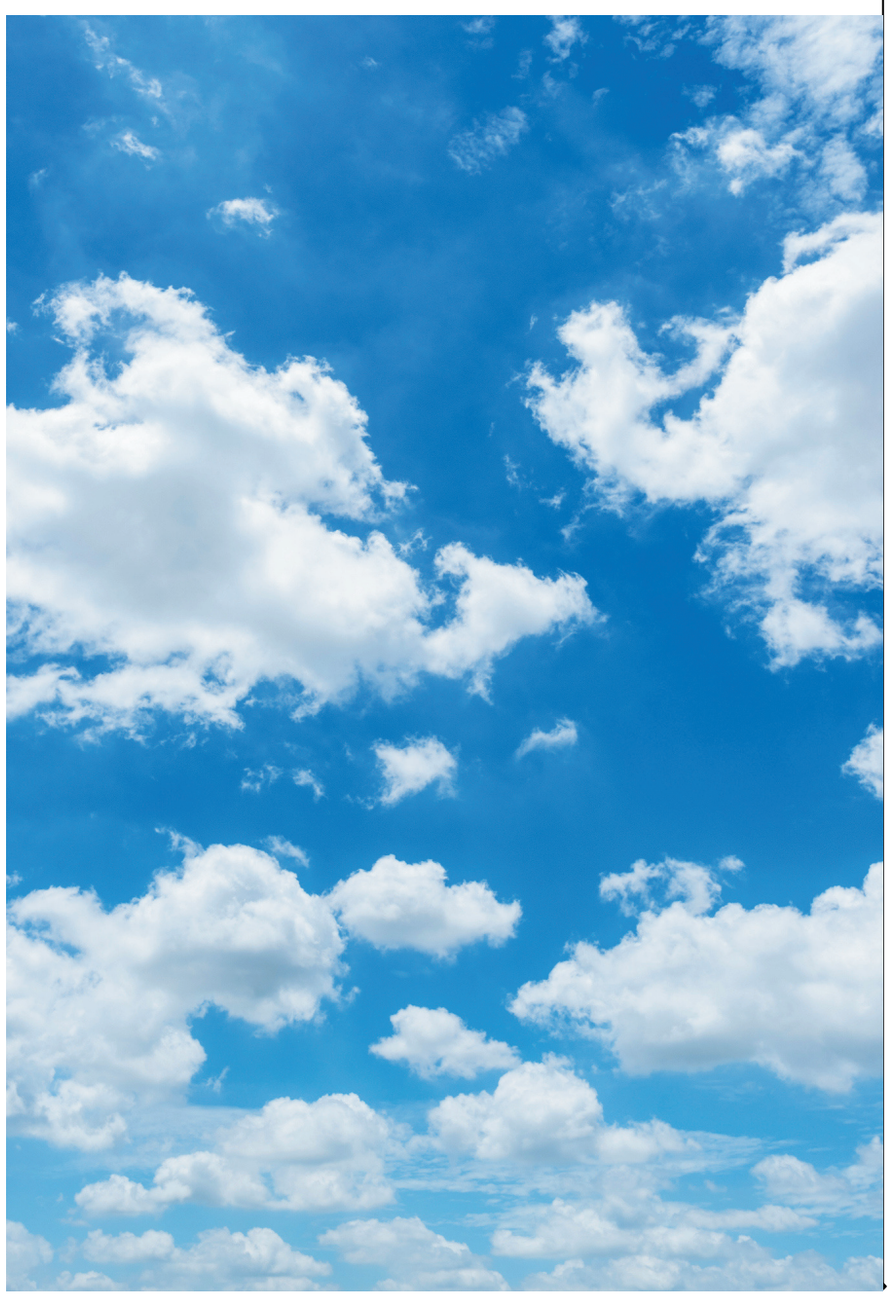
In both a recent interview for *Insurance Times* and a company thought leadership article, Intersys MD Matthew Geyman highlighted the growth of the chief AI officer role across many industries.

Matthew focused on both the business advantages of AI and the potential pitfalls, commenting, 'Using AI in businesses is like walking a tightrope between colossal opportunity and an equally large information security risk.'

While highlighting the potential for AI in financial services in areas such as loss and risk modelling, and interacting with customers, he also revealed concerns about incorrectly deploying AI and the dangers of inadvertently leaking classified data.

He said, 'If you're implementing AI at pace, assigning a chief AI officer could and quite probably should be considered an urgent matter.'

CLOUDY, WITH A CHANCE OF RADICAL INNOVATION



Financial services firms are increasingly using cloud services as a means to harden security and transform their digital infrastructure. The transition to the cloud comes in the wake of regulatory fines for breaching data regulations, such as the $3m imposed by Swedish body the Authority for Privacy Protection on insurer Trygg-Hansa.

Moving to the cloud offers opportunities for rejuvenation and innovation, for instance by integrating AI or Internet of Things technologies into operations. By updating ageing networks, it can also be a route to robust cyber security.

As a recent post on the Intersys website points out, 'The cloud can accelerate the time to market for new products or services, reduce the cost to serve, enable economies of scale and provide access to capabilities that are impractical, expensive or impossible to host on-site.'

However, a cloud migration must be undertaken by a partner with an understanding of the financial services sector and its rigorous data protection regulations.

With its knowledge of the insurance sector and its compliance credentials – including a recent recertification to the updated ISO 27001:2022 standard and Cyber Essentials Plus certification – Intersys provides secure and compliant cloud migrations for financial clients.

YOU *MUST* INSIST ON NIST



Jake Ives, Head of Security at Intersys, is calling on more organisations to put the NIST Framework front and centre of their cyber security strategies.

NIST is the USA's National Institute of Standards and Technology, and its Cybersecurity Framework is considered the leading global standard for cyber security best practice. It features five categories: **Identify, Protect, Detect, Respond** and **Recover**, with a series of suggested activities for each. While implementing the detail of NIST is the responsibility of IT and cyber security teams, Jake says that the general principles should be known – and discussed – at leadership team level.

He says, 'Because NIST is based on broad precepts, even laypeople can understand it and use it as a benchmark for measuring the performance of a cyber security provider. In fact, I highly recommend they do just that.'

ADVERTISEMENTS:



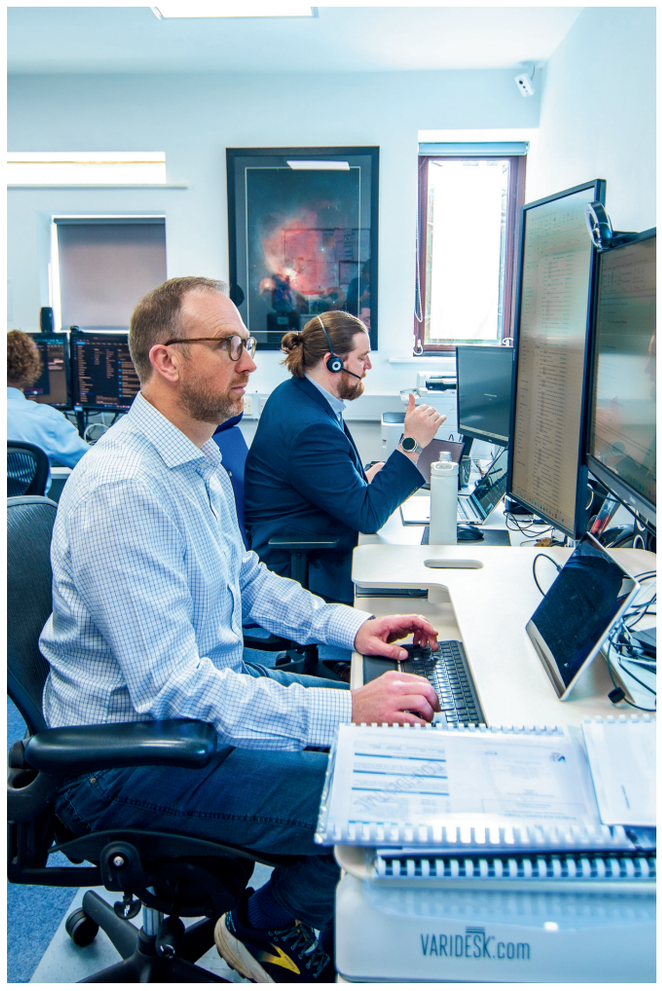












WHO IS NEW IT PROVIDER FOR THE CITY OF LONDON?

Intersys' MD Matthew Geyman has announced 'huge satisfaction' at his business' return to the City of London, where its story began.

In the mid Nineties, Matthew was an IT manager for an insurance underwriting company in the City when he saw an opportunity to start his own IT consultancy and outsourcing business. He began Intersys in 1996 as a one-man operation, traversing Central London on a Triumph motorbike, so he could serve as many clients as possible.

The company grew steadily and now has 45 employees and over 120 clients. Throughout, the business has maintained a close connection with the City, serving clients in insurance, fund management, fintech and more.

The leadership team also includes Head of Software Development Tony Healey, who started his career in the London insurance market; Malcolm Alexander, non-executive director, who headed the IT company that pioneered electronic trading; and Catherine Geyman, Director of Risk, who has a background consulting financial clients in risk management.

The business has maintained an impressive roster of long-term clients (see 'Intersys Clients 10X Less Likely to Suffer Cyber Attack' story, page 1) due, in part at least, to its service-over-sales ethos. It has also resisted the trend to outsource support to foreign providers, which can compromise service and security.

Says Matthew, 'Long-term relationships, trust, and clear and fair billing policies are the values we live by. As well as visionary IT and cyber security, of course. It's a straightforward approach, it sits well with me and the team, and our success over the years shows that it works.'



EXCLUSIVE: BARRY CADSHAW'S DIARY

In an exclusive extract from his diary, cyber sec guy about town Barry Cadshaw gives his take on staying safe in the City, both on and offline.

'As I sit at my laptop, I can't help but wonder: in a world where we share our personal profiles, photos and deepest inner thoughts online, how much are we really protecting ourselves?

'We put so much trust in the internet, but with hackers and data breaches becoming more common, it's hard not to feel vulnerable. I mean, if giant corporations with all their resources can't keep their information safe, what hope do the rest of us have?

'But then I realised: it's not about being completely invincible, it's about being smart and taking precautions. We lock our doors and set our alarms, so why not do the same for our virtual lives? It's time to start taking cyber security seriously, because in the end, our online presence is just as much a part of us as our physical selves. So here's to being safe, both on and off the screen.'

Important note: Any similarity between the 'Cyber Sec and the City' gang (left) and Intersys team members is purely coincidental. Friends of Intersys who insist on pointing out an uncanny resemblance may be met with repeated and not very convincing denials.



CLIENTS PRAISE INTERSYS' APPROACH

'Our management framework required considerable expertise and Intersys did a great job. I could certainly recommend their service.'
Citadel Risk

'Our firm needed to audit our cyber security capabilities. We are now able to confirm with confidence the standards we have achieved in partnership with Intersys.'
Global capital management firm

'The best IT company I have worked with in London! Reliable, professional, committed. The whole team at Intersys has high expertise in the field.'
Hedge fund



GET MORE IT AND SECURITY UPDATES

Visit www.intersys.co.uk/blog to get the latest information about cyber threats, best practice security, emerging regulations, Microsoft products and services that can help you work more safely and efficiently. You can also **subscribe to our security newsletter on the website** to get regular updates on current threats and the actions you can take to protect your organisation. Finally, take a look at **our LinkedIn page at https://www.linkedin.com/company/intersys-uk/**. You'll discover quick security updates, and links to our latest posts and thought leadership articles from the senior Intersys team.

CONTACT THE INTERSYS TEAM

If you'd like to discuss how we can help you leverage your IT and mitigate cyber risks, call us on +44 (0)20 3005 4440 or email info@intersys.co.uk. We'll introduce you to a senior team member who understands the unique challenges of your sector.

