FREE
PLEASE TAKE A COPY

IT & Cyber Times

BROUGHT TO YOU BY
INTERSYS.uk
IT Services and Security

IT & CYBER SECURITY NEWS FOR THE (RE)INSURANCE SECTOR

NO.2 SPRING 2025

‘DEAR INSURERS, GET CYBER SECURE’

The Bank of England Prudential Regulation Authority (PRA) published a ‘Dear CEO’ letter in January outlining its supervisory priorities for the UK insurance sector, with a strong focus on cyber security.

By March 2025, it expected firms to ‘have made significant progress already to strengthen their response and recovery capabilities to address cyber threats, remediate vulnerabilities exposed by legacy infrastructure and develop contingency procedures where material third-party services are disrupted’.

The letter put particular emphasis on operational resilience in relation to third parties, urging ‘robust oversight of their major outsourcing and third-party risk management providers’. This echoes the regulations introduced by the EU’s Digital Operational Resilience Act (DORA), reflecting the rapid growth of ‘back door’ cyber attacks on institutions via third-party partners.

Says Intersys’ Director of Enterprise Risk Management, Catherine Geyman, ‘This letter shouldn’t come as a surprise, because timelines for improving cyber security were on the table. I am, however, encouraged by the focus on third-party risk – this is a vulnerability that needs addressing for many insurers.’

INDUSTRY VOTES CYBER CRIME AS SECOND BIGGEST RISK AFTER AI

Cyber attacks and outages came second only after artificial intelligence adoption in the workplace in a recent industry survey on risk in insurance. Global insurance law firm Kennedys asked its partners to rank 10 risks, with more than 170 partners in 17 countries responding. While AI adoption in the workplace came top, cyber attacks were considered the greatest threat in the immediate future, especially given the AI tools now available to criminals.

These tools have expanded the attack surface and are increasingly being used in social engineering, malware and chatbots. For some time now, even novice criminals have been able to launch sophisticated attacks using ‘phishing as a service’ software. AI will only further increase their reach and effectiveness.

Full results of the Global Survey Risk Ranking, in order of severity were: adoption of AI, cyber attacks or outages, extreme weather, geopolitical instability, economic volatility, social inflation, use of evolving tech, shifting regulatory landscapes, civil justice reforms and increased focus on sustainability.

LONDON MARKET CABLE ATTACK A WARNING, SAYS INTERSYS CEO

The recent attack on fibre-optic cables in the London Insurance Market is a reminder that operational resilience must address both physical as well as cyber risks, says Intersys MD Matthew Geyman.

Quoted in *The Guardian*, *Commercial Risk*, *Insurance Edge* and *Insurance Times*, Geyman noted that the attacks, which occurred on 20 January, did slow down internet speeds in the City of London but appeared to have led to very little significant disruption.

He said, ‘This either speaks highly of the preparedness of the organisations involved and their business continuity planning (BCP) or means they’re excellent at remaining tight-lipped.’

This attack, which was undertaken by climate activists, was repelled most likely because many businesses have invested heavily in refining their BCP and disaster recovery (DR) plans, especially following the pandemic.

However, the incident does underscore that digital transformations in the market must emphasise resilience – and a holistic approach is crucial, with an emphasis on physical infrastructure risks as well as the cyber variety.

Says Geyman, ‘Highly coordinated attacks like this should encounter multiple layers of redundancy — from alternative fibre routes to wireless and radio link backups — designed to limit the impact of severed connections.’

In the weeks following the attack, Intersys has kept a close eye on further developments. During a briefing on 20 February, the City of London police shared a link from newspaper *The Prisma*. It spoke to Shut the System (STS), which claimed responsibility for the attack. According to the newspaper, ‘Their main target right now is the insurance industry.’

‘This insight from the police only reinforces the need for redundancy,’ says Geyman.

AI REGULATION DIVIDE IS NOT GOOD FOR INDUSTRY

Intersys' Professional Services Director Mark Kirby has warned that the UK and USA's refusal to sign the Global AI Declaration poses risks for businesses – and in particular the insurance industry. Kirby's comments to *Insurtech Insights* comes after over 60 countries endorsed the declaration on 11 February.

AI continues to develop and be adopted across the globe in more and more industries. However, the absence of clear regulatory frameworks presents liability, compliance and cyber security challenges. Meanwhile, the insurance industry is under increasing pressure to assess and mitigate AI-related exposures. Many believe that the Global AI Declaration would have helped to establish norms and standards for AI development in the future.

Providing it was widely embraced, the declaration would have helped create standardised regulations across jurisdictions and consistent risk management strategies.

In the article, Kirby (pictured below centre) spoke about the dangers of AI to insurers. This includes bias in training models, something which can lead to inaccurate underwriting and claims assessment decisions. Other risks include AI-related fraud such as deepfake-enabled scams and hyper-personalised phishing attacks.

He said, 'The industry must prepare for these challenges. The failure to establish international AI standards only increases exposure, making it imperative for insurers to integrate AI risk management into policies, fraud detection and cyber liability coverage. Insurers simply cannot afford to wait for governments to catch up.'

IT'S GETTING PERSONAL: HOW EMPLOYEES CAN (AND MUST) PROTECT PRIVATE DATA

The government's push for access to personal data to power the economy led to a row with Apple in February. As a result, the tech firm withdrew a security tool from the UK which provided end-to-end encryption of sensitive data.

With the debate about future use of our personal data continuing, this is a good time to remind ourselves of a particular risk to businesses – namely that work from home and BYOD policies bring our private and work lives uncomfortably close together. Encourage good personal data hygiene among your workforce with these tips .

• Only enter information online on sites that begin with https://
• Always use a virtual private network (VPN) when connecting to public networks
• Remove your information from public databases using services such as https://incogni.com
• Sign up for the telephone preference service
• Change your Wi-Fi password as soon as you receive your router
• Place IoT devices on a guest network to segregate them from your main (computer) network
• Don't buy cheap electronics such as routers, IoT devices, or personal devices from lesser-known brands

You'll find much more detail about these tips and more on a recent Intersys blog post about World Data Protection Day.

NEW FINANCE DIRECTOR FOR THIS GROWING IT AND CYBER RISK PROVIDER

Intersys Limited has announced the appointment of Claire Geyman as Director of Finance and Commercial Excellence. Her arrival coincides with the steady growth of the cyber risk and IT provider both in the UK and globally, and she will be at the helm of long-term growth strategy.

Claire arrives at Intersys after a successful career at Coloplast UK. In her role as Head of Finance and Commercial Excellence for North Europe Region, she was responsible for 14 countries and six reporting units, across seven currencies. Prior to her work at Coloplast UK, she held a variety of finance roles at blue chip organisations.

Her duties at Intersys will include informing business strategy through data-driven decision-making, business analytics, formulating sales and marketing objectives, pricing, wholesaler management, business intelligence, sales capacity analysis and developing and refining operating models.

'An exceptional team'

Announcing her arrival, she said 'Intersys is a family-run business whose values strongly resonate with those I've cherished in my previous roles. They specialise in IT managed services, cyber security and risk management, and also offer customers an award-winning supply chain risk management software trusted by a number of Top 10 global pharmaceutical and insurance companies. I'm thrilled to join as Director of Finance and Commercial Excellence and to collaborate with an exceptional team.'

Claire brings a wealth of experience in finance and commercial excellence to Intersys. She holds a BSc in Economics and German and is fluent in the language. She started her career working in German operations for multinational organisations before qualifying as an accountant. Her career has included senior finance roles in various multinational corporations, eventually leading to her previous role as Head of Finance and Commercial Excellence for North Europe Region at Coloplast.

Growing family business

Since 1996, Intersys has grown from a one-man IT support service to a team of over 50. A recent expansion into Leadenhall Market, as well as global partnerships in India, Australia, New Zealand and other territories, reflects its increasing prominence as a cyber secure IT provider. Claire joins other Geymans – Matthew, Catherine and Richard – in this family-led business.

> "I'm thrilled to join Intersys Ltd and to collaborate with an exceptional team"
>
> **Claire Geyman, Intersys**

IT'S TIME TO FACE REALITY, INSURERS: YOUR LEGACY SYSTEMS ARE A TICKING TIME BOMB...

Ignorance, as the saying goes, is bliss. But perhaps not in the world of insurance cyber security. The sector is a data goldmine for criminals. And, disconcertingly, they may sit on stolen data for *months or years* before launching an attack. As former Cisco CEO John Chambers said, 'There are two types of companies – those who have been hacked and those who don't yet know they have been hacked.'

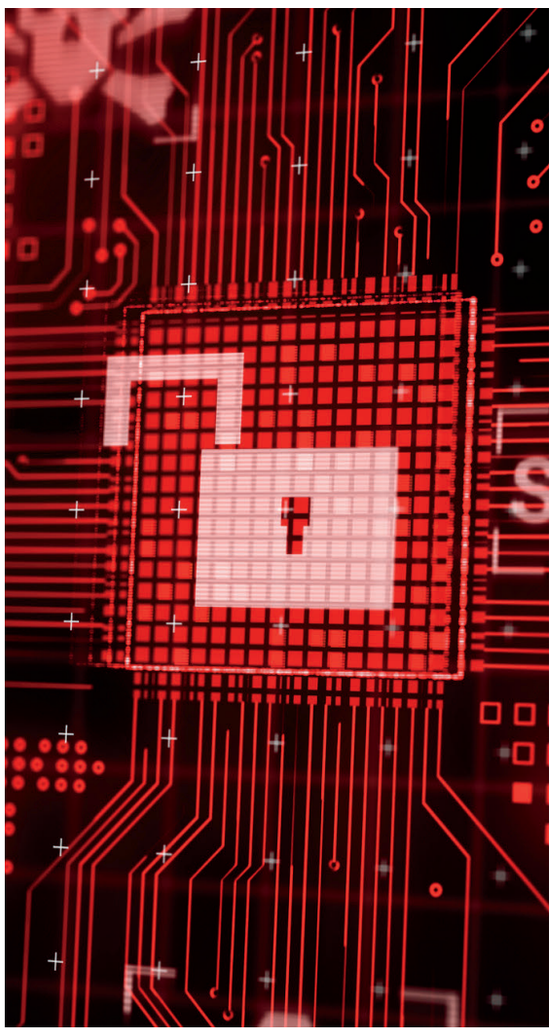
Intersys recommends several strategies for insurers to determine if their business has been breached and to check that data is being protected correctly.

A fundamental step is locating possible incursions. Your IT department should retain access logs to track what is being accessed and when in the event of a breach. Ideally, these should be monitored with automated alerts to flag unusual activity.

You should also check what information about your company is online. Intersys offers a free tool to insurers which generates a report of everything linked to your company. Ask us to send you the tool so you can find out what people know. This can help to inform any need to update logins.

Old systems, new threats

We also need to talk about legacy proprietary insurance systems. Many carriers operate on decades-old infrastructure that wasn't designed with modern cyber security threats in mind. With the threat increasing, now is the time to ensure you implement comprehensive secure lifecycle management. This includes deploying vulnerability scanning tools on every major release, regularly testing for weaknesses and maintaining robust update protocols.



Says Intersys' Head of Software Development Tony Healey, 'As cyber threats evolve, the traditional "set and forget" approach to insurance technology becomes increasingly dangerous. It potentially exposes sensitive client data and creates substantial business interruption risks that could devastate balance sheets. You must monitor and update systems regularly.'

Visit www.intersys.co.uk/blog for more advice about cyber security best-practice, emerging threats and keeping your business safe online.

HOW THE MGA SECTOR IS GETTING CYBER SECURE

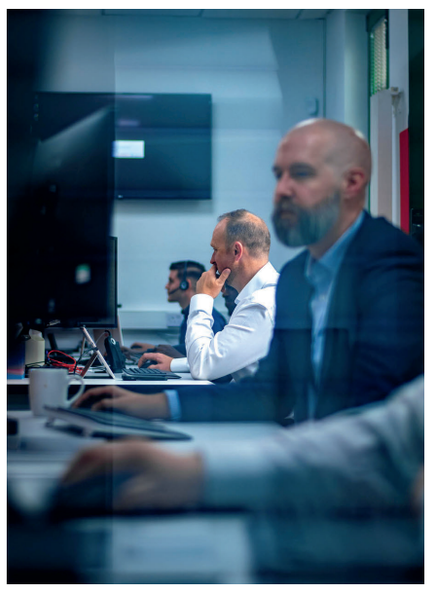
In a recent article for *Resilience Forward*, Intersys MD Matthew Geyman highlighted the growth of the virtual chief information security officer (vCISO) model in the managing general agent (MGA) sector.

The sector, which generated $23.9 billion in global revenue in 2023, faces increasing cyber security challenges as its rapid growth attracts more criminal attention. Incidents like CNA Financial's £30 million ransomware payment and the widespread breaches affecting insurers globally serve as stark reminders of the vulnerabilities inherent in the sector.

Says Geyman, 'As MGAs integrate new vendors, clients and platforms, their third-party risk increases with each integration. For mid-sized insurers and start-up MGAs, developing resilience against these threats is no longer optional – it's an urgent necessity.'

The vCISO model provides flexible, scalable cyber security leadership, particularly beneficial for MGAs operating with limited resources.

Geyman explains that this approach allows companies to implement robust security measures while continuing to maintain their growth trajectory. He says, 'The vCISO model isn't just about cost savings; it's a strategic and necessary investment in a firm's future.'



CYBER ESSENTIALS: CLUE'S IN THE NAME

Senior Engineer at Intersys James Day is calling on more businesses in the (re)insurance sector to attain Cyber Essentials certification.

Cyber Essentials is a certification scheme backed by government to help organisations keep their data – and customers' data – safe from cyber attacks. The UK government's National Cyber Security Centre states it is a minimum standard of cyber security for all organisations – from SMEs to large corporations.

Says Day, 'I encourage uptake by saying "the clue's in the name". Getting certified is an essential step for any insurer or reinsurer in the UK and if you don't have Cyber Essentials yet, you should start investigating the process right away.'

Cyber Essentials (Basic) is a self-assessment certification. Your organisation must verify it has fundamental security controls in place across five key areas: firewalls, secure configuration, user access control, malware protection and security updates. Cyber Essentials Plus includes the above, along with independent assessment.

Intersys offers a Cyber Essentials Assessment service to audit and align businesses with standards and guide their application.

ARE YOU SECURITY SAVVY?

Think you're hard(ened)? Try our quick quiz

1) You receive an urgent email from your CEO asking you to transfer £1 million to a new account. What next?
a) Call the CEO to verify the request.
b) Reply to the email just to double check that it's legit.
c) Assume your CEO has finally noticed your excellent work and is rewarding you with responsibility.

2) You spot a USB stick in Cheese at Leadenhall Market. Your next move?
a) Pocket it and forget about it until you find it in the washing machine.
b) Leave it in situ and report it.
c) Plug it in - maybe it contains Bitcoin!

3) Your underwriting colleague needs urgent access to the treaty system while working remotely. You should:
a) Grant temporary access using your credentials. Just make sure to change your password immediately afterwards.
b) Set them up with proper credentials and MFA through IT, following protocol.
c) Simply send your logins via WhatsApp. It's secure, right?

4) What's the smartest way to look after passwords for multiple reinsurance platforms?
a) Create a secure spreadsheet with all passwords, protected by encryption.
b) Use a company-approved password manager with strong unique passwords.
c) Write them in your paper diary labeled 'Top Secret Passwords'.

5) The best way to explain cyber aggregate exposure to your retrocessionaires is:
a) Through detailed technical analysis and exposure mapping.
b) 'It's like a really bad hurricane, but inside your computer.'
c) Drinks at Old Tom's Bar in Leadenhall Market followed by interpretive dancing.

ANSWERS: 1 a; 2 b; 3 b; 4 b; 5 a.
(If you got more than a couple wrong, consider reporting yourself to security.)

'WHAT WE DO IN THE SHADOWS' POSES MAJOR SECURITY RISK

In an upcoming thought leadership article for a UK insurance industry publication, Mark Kirby, the Professional Services Director at Intersys, has warned of the significant dangers of 'shadow IT'.

The name refers to any IT used within an organisation that isn't officially authorised. Insurers, like many businesses, often discover employees using unsanctioned software to process claims, communicate with clients, or manage workloads

The reason is sheer convenience, because secure, approved systems can sometimes be clunky or inefficient compared to non-approved platforms. However, unless the correct measures have been implemented, these tools are not subject to the same security controls as approved applications.

Says Kirby, 'A single compromised third-party app can serve as a gateway to a company's most sensitive systems. To counter this, insurers must strengthen their zero-trust frameworks and ensure strict visibility over all digital tools being used within their organisation.'

STATE SPONSORED ATTACKS: HERE'S HOW YOU CAN FIGHT BACK

Jake Ives, Head of Security at Intersys is urging businesses to develop greater awareness about the threat of state-sponsored attacks online.

He says, 'The impact of wider global conflicts is also going to be felt on our shores. We have seen how cyber crime groups with ties to Russia, China and other hostile states have consistently tested our security defences this last year. We should expect more of the same in 2025.

'Britain's cyber security chief Richard Horne has already warned that hostile activity in cyber space went up by 16% in 2024 alone. These figures are worrying but there are steps that organisations of all sizes can take to shore up their security.

'I would recommend fundamental exercises such as gap analysis and cloud security reviews to understand your current security posture. Then, implementing security controls such as DMARC (to prevent email spoofing) and conditional access polices in MS365 (to ringfence sensitive data and applications) are crucial. Regular penetration tests can also expose unknown security gaps in your systems. Finally, a continued programme of user education and awareness is essential to ensure a culture of security within the organisation.'

And that LinkedIn post on the topic du jour? Jake recommends caution. 'Posting your personal political views on LinkedIn can give politically motivated hackers more of a reason to target you and your organisation.'

In his Cyber Security Year in Review, available on the Intersys blog, Jake also looked at other security trends, including the rise of malicious AI-driven cyber attacks and the continued presence of ransomware as a major cyber crime. Cyber Essentials certification was, he said, a vital step in becoming secure.

CHEESE, FINE WINE AND CYBER CRIME

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 firm. He began Intersys in 1996 as a one-man operation, weaving through Central London on a Triumph motorbike, so he could serve as many clients as possible.

The company grew steadily and now has over 50 employees and more than 140 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 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 Enterprise Risk, who has a background consulting financial clients in risk management.

LONDON MARKET PRAISES INTERSYS

Intersys has received the seal of approval from well-known names in the London Market.

Says Human de Jager, Head of Information Technology at Dynamo Analytics, 'Our business has expanded rapidly and it's been hugely reassuring to know that our IT and cyber security provider has many years of experience – over 25 in total – working with financial clients.

'At every turn during our growth, Intersys has provided us with solid strategies for scaling up our IT estate and hardening our security in a way that keeps us compliant with domestic and international financial regulations. To complement this, they always "have our backs" if we need strategic advice on specific areas – our ISO 27001 and Cyber Essentials certifications being good examples. Great service. Friendly team. Highly recommended.'

Meanwhile, Mike Palmer from Citadel Risk says, 'Intersys did a great job of gathering all the necessary data about our company's global systems and processes, and then benchmarking it against the expected standards. I could certainly recommend their service.'

Intersys has worked with City clients for nearly 30 years, including ACORD, ACORD Solutions Group, Citadel, Dynamo, Ebix, Munich Re, Operational Risk Consortium (ORIC) and Pharmaceutical Captives.

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, and 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 receive 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.

SECURE ♥ CONNECTIONS

Insurance professionals seek cyber-secure IT partners

LONELY UNDERWRITER LOOKING FOR COVER Well-capitalised, loss-adjusted professional seeks a stable risk profile. Loves long walks down Lime Street, cyber resilience and mutual indemnity. Let's negotiate favourable terms over drinks at the Lamb Tavern.

CLAIMS EXPERT READY TO SETTLE Fully reinsured against heartbreak, but willing to take a calculated risk. Genuine kind of chap, seeking multi-factor authenticity from a reliable partner. Meet me near The Royal Exchange for due diligence over drinks.

WILL YOU BE MY FIREWALL? It's tough out there and I've been burnt in the past. Looking for a strong partner to shore up my defences and harden my security. Me and you, versus the whole damned world? Let's build a beautiful firewall together...

SEARCHING FOR MY SILVER LINING Regulatory capital specialist experiencing server-based data drudgery. Looking for a cyber-resilient IT provider to sweep me off my feet and put my head in the cloud. Let's talk Azure at Osteria Del Mercato. Ethical partners only – no bad actors.

I WANT TO GROW WITH YOU Claims director tired of cyber security providers with all the loyalty of a tindr addict. I want to negotiate a partnership high on mutual benefit and longevity. Is their life beyond the IT churn? Meet me at the corner of the Intersys office, Leadenhall Market...

CONTACT THE INTERSYS TEAM

Call us on +44 (0)20 3005 4440, email info@intersys.co.uk or simply drop in at 1st Floor, 29/30 Leadenhall Market, City of London EC3V 1LR. We look forward to meeting you and providing specialist IT and cyber security advice for the (re)insurance sector.