

# Defensive lines

Understanding how to  
better prepare and respond  
to a cyber attack

Start



Mills & Reeve and Aon surveyed legal, risk, compliance and human resources teams in the private and public sectors, across a wide range of industries, to better understand how they prepare and respond to cyber attacks.

The findings presented in this report are a stark reminder of the size of that threat and the impact cyber attacks can have. Attacks can come from many sources, from organised crime, to terrorists, hackers or hostile states, and in many forms, from ransomware and phishing, to spoofing, or man-in-the-middle attacks.

Half of all organisations that were surveyed for our report have experienced a cyber attack in the past 12 months, with one-third experiencing multiple attacks. Those organisations that have not been attacked should consider themselves lucky as it seems that it is very much a case of ‘when’ rather than ‘if’ a cyber attack will occur.

The risks facing organisations have never been greater. An economic downturn may see less investment in technology, IT security and compliance activity. That sits alongside the largest shift in working patterns in a generation, with a corresponding increase in remote access to key business or organisational systems through the increased use of Cloud Computing (and, in particular, Software as a Service or ‘SaaS’ solutions). And then there is increased activity from state-sponsored cyber criminals, with concerns being raised particularly about prospective threats from countries such as Russia, North Korea and China. Organisations face a perfect cyber storm.

Now is not the time for complacency. It is a time for heightened readiness, to review and strengthen preventative measures, and to stress test responses.

This report highlights some of those risks and how organisations are responding. It is prudent business practice to invest in preventative measures to minimise the risk and impact of a cyber attack, and so we also offer guidance and direction on what we consider best practice.

We hope you will find this report helpful and engaging, and please do contact us should you wish to discuss any of the issues we raise. Contact details can be found at the end of the report.

This report is based on over 130 interviews with Mills & Reeve and Aon clients in legal, risk, compliance and HR teams in the private and public sectors, across a wide range of industries, in Q4 of 2022.





### Cyber attacks are here to stay

95% of business leaders we heard from are either concerned or very concerned about cyber and data security.

### Operation or reputation?


The ability to continue to operate following a cyber attack is the main concern for 53% of organisations surveyed, with 38% primarily concerned with reputational damage.

### No confidence

Legal, IT and risk teams — internal cyber function teams — are approximately twice as likely to confirm ‘no confidence’ in identifying the consequences of a cyber breach and the mitigations within the regulatory 72 hour notification period as those not responsible.

### Ransomware confusion

It’s headline news, but there is a lack of consensus as to approach. Although just 2% of organisations we contacted openly said they would pay ransoms following a ransomware attack, the rest are divided as to whether or not they would. 26% said they would do what their IT teams tell them, 24% would be led by their insurers, and 21% would be led by their legal teams.



### Disconnect in approach

There is a surprising degree of disconnect in approach to cyber risks with 47% of organisations we surveyed not working collaboratively to protect against cyber attacks.



### Tick-box GDPR

There is a mismatch between the importance of GDPR compliance in guarding against cyber risks and liability, with a fifth of those we surveyed viewing it as nothing more than a tick-box exercise, something that gets in the way of day-to-day activity or a necessary evil.



### Training overlooked

The importance of data protection training in the context of cyber risk mitigation is being overlooked. About a third of organisations we surveyed are not undertaking the mandatory minimum frequency of data protection training.



## Cyber risk and preparation

Organisations are alive to the threat of cyber attacks, and so they should be. Our survey finds that 50% of organisations have suffered an attack in the last 12 months, with a third of those reporting multiple attacks.

---

Organisations are alive to the threat of cyber attacks, and so they should be. Our survey finds that 50% of organisations have suffered an attack in the last 12 months, with a third of those businesses reporting multiple attacks.

Our survey also reports that 95% of organisational leaders are rightly ‘concerned’ or ‘very concerned’ about cyber attacks on their organisations. Just 5% state they are ‘not concerned at all’.

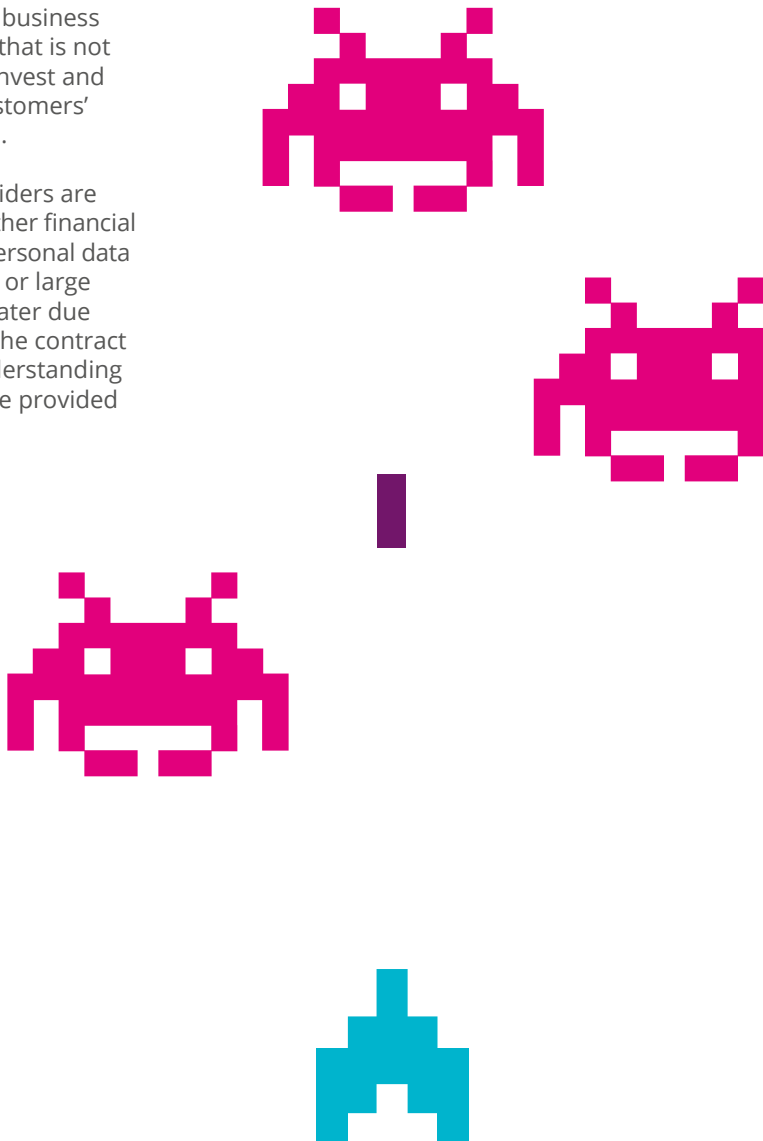
Some organisations have adopted strategies that see business critical functions outsourced to external suppliers. However, our findings have revealed that they have misinterpreted that as ‘outsourcing’ their management of cyber risk and data protection to the service provider as well.

It is an approach that leaves them exposed in the event of an attack and open to greater scrutiny and fines from the Information Commissioner’s Office (ICO). Ticketmaster, for example, was fined £1.25 million by the ICO when a chatbot offering by a third party service provider allowed cyber criminals to access customer payment details — the ICO’s fine made it clear that it did not entertain any prospect of ‘outsourcing of risk’ in that case.

Organisations are often mistaken in believing that responsibility for cyber risk and data management is passed on to a third party provider when business functions are outsourced. But that is not the case. Organisations must invest and take responsibility for their customers’ personal information and data.

Where third party service providers are processing sensitive data (whether financial data or ‘special categories’ of personal data related to health, for example) or large amounts of personal data, greater due diligence is needed as part of the contract negotiations, alongside an understanding of the way in which services are provided and delivered.

### How concerned about attacks is your organisation?



Whether holding too much data, keeping it for too long or changing working patterns, commonplace business practices are leaving organisations unnecessarily exposed should they fall victim to a cyber attack.

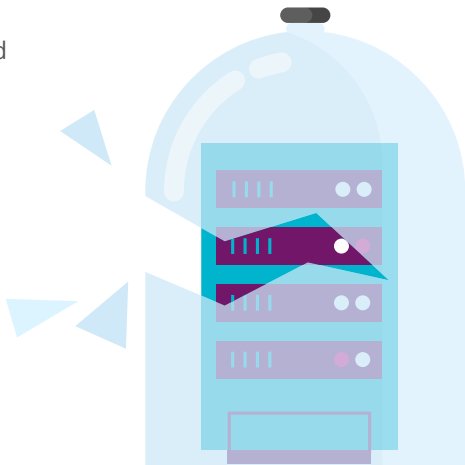
However, in many cases they can be easily addressed, with GDPR providing the framework to work to.

It's encouraging then that most respondents view the GDPR regime as essential to protecting individuals' personal data. A culture of genuine concern will give confidence to customers, suppliers and employees that their personal information is valued and treated accordingly.

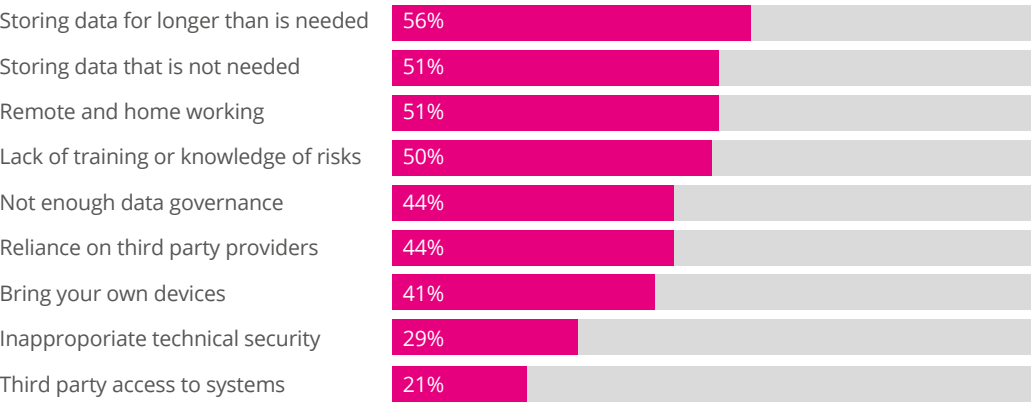
Unfortunately, almost a third of respondents to the survey see it as nothing more than a compliance-led requirement and, of greater concern, a fifth continue to see GDPR as

nothing more than a 'tick-box' exercise or something that gets in the way of day-to-day activity, or is a 'necessary evil'.

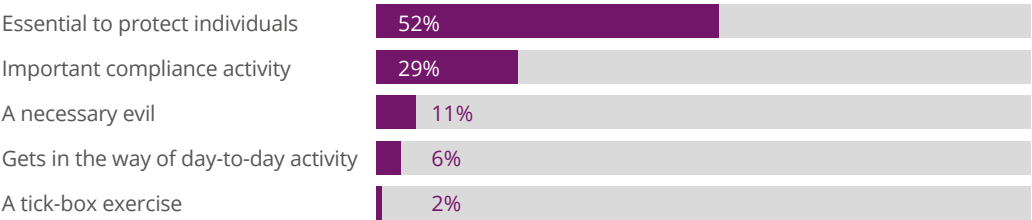
Relegating GDPR to a simple 'moment in time' activity, or worse, not taking it seriously at all, is a weak foundation on which to build a customer and staff centred culture. Cracks will appear and can all too easily be exploited by sophisticated cyber criminals.



## Nine ways businesses increase their exposure to cyber risk



## How does your organisation view GDPR compliance activity?



The key GDPR principles, if truly embraced, can be extremely valuable to guard against cyber risks.



**Jagvinder Singh Kang**  
Head of cyber response  
Mills & Reeve

**Data minimisation** — the more information which an organisation has about an individual, the greater the scope of harm to that individual should the information end up in the wrong hands. Therefore, collecting the minimum amount of information to fulfil an organisation's purpose reduces cyber risks.

**Storage limitation** — keeping information for no longer than is necessary removes it from the scope of a cyber attack and reduces risks accordingly.

**Integrity and confidentiality** — using both a technical (eg, encryption, multi-factor authentication, anti-malware safeguards) and organisational approach to guard against unauthorised access to personal data provides better safeguards against cyber risks.

**Lawfulness, fairness, transparency and purpose limitation** — having a focus and transparency at the outset as to how personal data is going to be used and

shared guards against scope creep. This also avoids the data finding its way into unintended systems and uses where it is susceptible to attacks.

**Accuracy** — with the increased risks of 'spoofing' by cyber criminals, it is important that individuals' records are kept up to date, especially when such data is used for identity checks or for communicating with individuals.

**Accountability** — undertaking data protection impact assessments helps an organisation to detect and mitigate vulnerabilities upfront.

As can be seen from these principles, cyber risk mitigation and GDPR compliance activities go hand-in-hand to safeguard an organisation from risks to personal data.

Over half of the organisations contributing to our survey recognise the potential of a cyber attack to impede ‘business as usual activity’, and over a third are alive to the possible reputational impact.

The prospect of a partial or full shutdown to an organisation is very real. Yet business continuity and disaster recovery measures are often ‘glossed over’ during contractual negotiations, or relegated to being simply a ‘schedule issue’ or something to be agreed post-contract signature. This is a high risk approach when it comes to mitigating cyber risks.

Organisations need to understand the business continuity and disaster recovery measures of their service providers, as well as the inter-play between internal and external measures. Exercises should be run by the parties to ensure that the measures will provide the intended outcome, rather than simply ‘hoping for the best’ should disaster strike in the form of a cyber or ransomware attack.

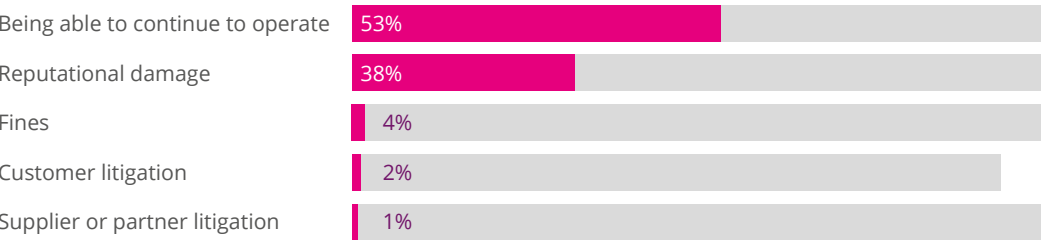
**Helen Tringham**, cyber litigation partner at Mills & Reeve, comments: “It is understandable that litigation is not the priority in the immediate aftermath of a cyber breach. The priority should be on business continuity and service delivery. However, organisations should not lose sight of the risk of litigation or regulatory action as, once the dust settles, the financial risk around litigation or regulatory action could pose the biggest financial threat to the organisation.”

In particular, organisations should be mindful not to lose the right to argue that certain communications sent in the immediate aftermath of a cyber breach are covered by legal privilege, to prevent them from being disclosed in court proceedings or regulatory action.

We often find that people may be less cautious in what they say and write in the immediate aftermath of a cyber breach — often allocating blame or accepting fault on the basis of an incomplete or inaccurate picture. Businesses should, therefore, proceed with care in such circumstances, to prevent unhelpful comments coming back to bite them in any future regulatory or legal action taken against them.



## What is your organisation’s main concern after a cyber breach?





Given the impact a cyber attack can have on an organisation, it should be natural to take a holistic view towards guarding against those attacks. Legal, IT, HR, business and communications teams should work together to ensure best practices and the appropriate response.

Yet, our survey reports that almost 50% of organisations do not have their IT and legal teams working collaboratively to manage and guard against cyber risks. A quarter of organisations say they do not know what approach their firm adopts in this regard.

That divide needs to be bridged. In particular, organisations need to find those intermediaries in IT and legal that can ‘speak the same language’ to each other to ensure a collaborative approach.

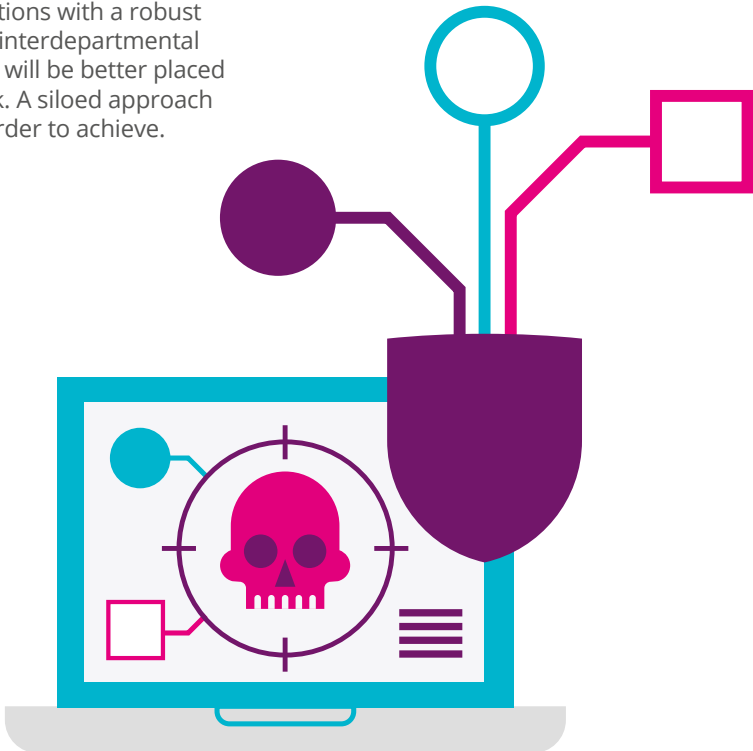
**Jagvinder Singh Kang**, head of the cyber response team at Mills & Reeve, comments: “Being both a technology lawyer as well as a qualified software engineer, I have often seen the challenges experienced by organisations when legal teams don’t understand the tech, or tech teams don’t understand the legal ramifications of what they are doing with the tech or outsourcing.

“Having technology lawyers who understand the tech and the law, whether internally within an organisation or by way of external advisers, is key to unlocking a siloed approach and bringing teams together to mitigate cyber risks and liability.”

It should go without saying that such individuals should be found proactively in advance of any cyber attack, as they may well not exist in many organisations. External specialist technology law advisers who also have technology credentials to understand the underlying tech are often well placed to step into that role.

Consequently, organisations with a robust culture of collaborative interdepartmental cyber risk management will be better placed to survive a cyber attack. A siloed approach will make that much harder to achieve.

## How do your teams work to protect against cyber attacks?



# Cyber response

Cyber attacks will take many forms, each presenting its own unique challenges. Yet it is ransomware attacks that are often the cause of much debate and frustration.



Cyber attacks will take many forms, each presenting its own unique challenges. Yet it is ransomware attacks that are often the cause of much debate and frustration.

Business critical IT functions are quite literally held to ransom and only released when a payment, typically via crypto assets, is made.

The question is whether to pay or not.

Our survey results suggest organisations are struggling with that decision. There is a difference in opinion, with 2% saying that they would definitely pay — this potentially indicates both business continuity concerns as well as reputational management concerns. A greater proportion of respondents, 27%, have said they would definitely not pay. The other respondents seem to be almost equally divided between taking the advice of their lawyers, insurers or IT specialists when dealing with ransomware attacks.

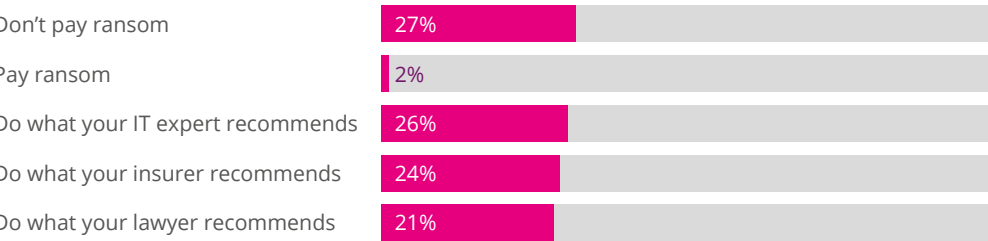
While the clear guidance from both The Law Society and the National Cyber Security Centre is that ransoms should not be paid, other considerations often have to be taken into account.

**Andrew Catley**, director – Stroz Friedberg Incident Response, Aon Cyber Solutions comments: “Whilst there are some very valid reasons for not paying a ransom demand, chief among them being the argument that it perpetuates the cycle of extortion as a means for criminals to make money, it’s important for each circumstance to be considered on its own merits. If you are an organisation that is wholly against the idea of paying a ransom for morality or other reasons, then preparation is key. You have to be able to respond to and recover from this type of attack to minimise business interruption should the worst occur from a sophisticated threat actor.

If you get to a point where you are not able to recover, quickly or at all, then the question of whether to pay or not to pay is somewhat answered for you. Can you or your shareholders accept a destruction of business value instead of paying a ransom. But again, each incident on its own merits, with a certain degree of flexibility built into the planning for such eventualities.”

Consequently, if your organisation is in the ‘paying the ransomware camp’ then that in itself highlights that your cyber preparation is lacking and in urgent need of addressing.

How would your organisation respond to a ransomware attack?



The nature and extent of an attack needs to be quickly determined before action can be agreed. Put bluntly, time matters.

The GDPR has prescribed a 72-hour period for regulatory notifications where the impact of a cyber attack meets the appropriate threshold for reporting. Where appropriate, affected individuals need to also be informed “without undue delay”.

Interestingly enough, the internal departments tasked with handling a cyber incident (such as legal, IT and risk) are, according to our findings, approximately twice as likely to doubt that their organisation can identify the consequences and measures for mitigation within the GDPR’s 72-hour time limit, compared to those in other roles who are not responsible for dealing with a cyber incident. This divergence shows that organisations may be taking ‘false comfort’ in their perceived cyber resilience.

A mix of voices and opinions is to be valued, but when against the clock, a bridge between those voices is needed. That bridge needs to speak the language of IT and legal and provide clear direction and guidance. Jagvinder Singh Kang confirms: “This bridging of IT and legal is necessary not only during the procurement of IT software, systems or services, but also when dealing with a cyber breach. Without an understanding of the combined IT and legal issues, an organisation cannot have an effective cyber response proposition.”

Unless the consequences of a breach and the steps to be taken to mitigate a cyber breach can be clearly and swiftly identified, organisations will lose the opportunity to minimise the damage to the company caused by the cyber breach.

Could you identify the likely consequences of a breach?



Could you identify the mitigation measures needed?

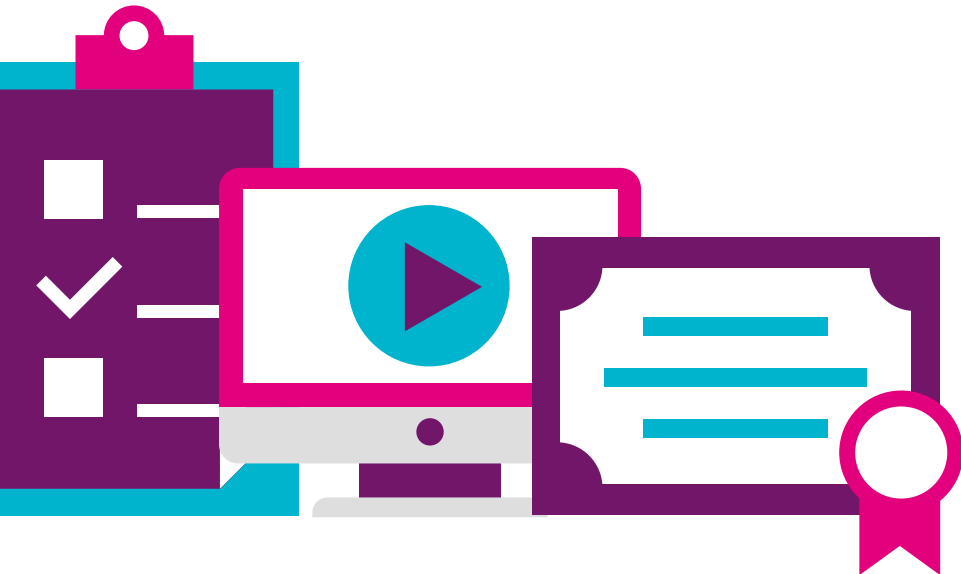


Our survey points to only 71% of organisations providing the minimum data protection training.

The lack of appropriate training is a gap in the corporate armour of organisations that cyber criminals will exploit. Furthermore, such a gap can be costly for organisations from a regulatory fine perspective, as has been apparent from the ICO fine issued to Interserve, where a phishing attack resulted in a £4.4 million UK GDPR fine.

Training should be provided to employees regularly, and in any event at least every two years. Training should make clear the steps employees should take to guard against cyber risks and how to report a breach should they become aware of one.

Employees can also be a direct threat. Companies need to be ready, not only to support employees affected by a breach, but also to act against them if they caused the breach. For example, when an employee takes personal data from the company, it may be appropriate to seek an injunction against them to recover the personal data in order to protect other employees and the business, and to mitigate any fine from the ICO or court action from affected employees.



“The biggest cyber risk businesses face is not from hackers outside of their company, but from complacency within their company. If your business doesn’t regularly monitor for suspicious activity in its systems and fails to act on warnings, or doesn’t update software and fails to provide training to staff, you can expect a similar fine from my office.”

ICO commenting in 2022 on the £4.4 million fine issued to Interserve for a cyber attack

The outcome of our survey provides a useful benchmark for organisations to take stock of their own preparation and response practices and procedures.

It is clear that cyber risks are something that no organisation can ignore, no matter which sector it operates in. However, a reactive approach will only yield limited results and will not be able to mitigate against, or avoid, the significant adverse practical and financial consequences associated with cyber.

A holistic approach which 'bakes in cyber protection' right from the procurement stage of systems and services through to ongoing systematic monitoring of arrangements, with a pre-built plan of the responses to take when a cyber attack materialises, is the best way forward.

Central to achieving this is having a collaborative approach with IT, legal and other business teams working collectively together. Where appropriate, internal teams should be supplemented by specialist

external IT and legal advisers who can help 'bridge any gaps' which may otherwise expose an organisation to heightened cyber risks.

One of the strongest weapons which an organisation can utilise to guard against cyber threats is a proactive UK/EU GDPR compliance strategy — but only where it is truly embraced by an organisation — as where wielded correctly, it can create a formidable defence in guarding against the risks and 'fallout' of cyber attacks.



**Mills & Reeve** is centred on achieving more for clients, their businesses and the wider communities we serve.

Our cyber response team can help clients proactively with cyber through our full range of legal services, including in respect of:

- Cyber strategy
- Regulatory cyber breach notifications
- UK/EU GDPR compliance
- Data Protection Impact Assessments
- IT systems or services procurement or supply
- Litigation and defence
- Reputation management
- Training



**Jagvinder Singh Kang**  
Head of cyber response

+44(0)7515 850 070  
[jagvinder.singhkang@mills-reeve.com](mailto:jagvinder.singhkang@mills-reeve.com)



**Helen Tringham**  
Cyber litigation expert

+44 (0)7484 075 631  
[helen.tringham@mills-reeve.com](mailto:helen.tringham@mills-reeve.com)

**Aon plc (NYSE: AON)** exists to shape decisions for the better — to protect and enrich the lives of people around the world.

Our colleagues provide our clients in over 120 countries and sovereignties with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.



**Andrew Catley**  
Director – Stroz Friedberg Incident Response, Aon Cyber Solutions

+44 (0)7824 547 805  
[andy.catley@aon.co.uk](mailto:andy.catley@aon.co.uk)