



Cyber security considerations in the public sector

Practical steps to protect yourself from a cyber attack

This week Trowers & Hamlins teamed up with Lloyds Bank and Gallagher to talk to a significant number of key players across the public sector about Cyber Security and what public sector organisations can do to protect themselves. The event was kindly organised by Lloyds Bank's Education, Charities and Government team and was really well received and offered some tips to deal with what is one of the most important issues for the sector. A brief summary is set out below for those who could not make it.

The key message was prevention is better than cure. Speak to anyone involved in cyber security and they will tell you that it is a question of when your organisation will be targeted rather if. There are many terrifying statistics about how likely an organisation is to be a victim of a cyber incident, how many security breaches there are, how many records are accessed or how much money is diverted by threat actors each month. The ways in which organisations are being targeted continues to evolve. The consequences of a cyber incident can be catastrophic for an organisation - it can cause numerous problems including financial, operational, regulatory, reputational and legal issues. It can take a long time to recover from a cyber incident and some organisations do not make it.

There are some simple things that every organisation can do to protect itself against an attack and to be ready should the worst happen:



Plan

Risk assessment, policies, a cyber response plan and insurance are really important things for all organisations to consider as part of its cyber tool kit. Having these in place mean that you will be as ready as you can be in terms of identifying your organisation's vulnerabilities and addressing those by setting policies and processes that are followed and tested. Specialist

cyber insurance can be a really good option to cover the risks you cannot eliminate and can offer financial protection up to the limit of your policy. When choosing your insurers, look out for true specialists - Gallaghers can also offer a wealth of experience in helping to identify risks and minimise those risks that organisations face. Finally, a cyber response plan that is tailored to your organisation is an absolute must. The worst time to consider how you might respond to a cyber incident is once it has happened. A cyber security incident is fast moving and you must act quickly and effectively to mitigate the damage and be in a position to respond to any regulators, your staff, your stakeholders and any other third parties. You need an experienced legal team and cyber specialists to be ready to work along side you if the worst happens. Trowers & Hamblins regularly work with clients in preparing for a cyber security incident and responding to them.



People

Despite any organisation's best laid plans and defences, it's people are usually the weakest link. A high standard of cyber hygiene across your organisation is essential but it is difficult to maintain. People are busy and have 100s of interactions with technology a day. It is easy to make a mistake - to be careless with your credentials, to click on a suspicious link or to fail to notice the slightly unusual format of a rogue email asking you to transfer money. It is essential to train your people and keep training them and make them as aware as possible of the sorts of things they need to look out for. Regrettably, cyber criminals will continue to come up with new ways of trying to break down our defences - organisations need to educate their people to try and keep up and remain vigilant.

Posture

Good cyber security posture is essential. Threat actors will only find ways into your system if you leave a door open. It is essential to have robust technology, processes and security systems around your servers and networks - just as you would with your office building or your home. The challenge for organisations is keeping up - it is time consuming and cost money. In circumstances where there is a strain on already tight budgets, it may seem like a difficult choice to prioritise this. However, the consequences of a significant incident more than justify the cost.

If you would like to discuss any of the above further or any other concerns, please do not hesitate to get in touch with any of our specialists.

Key contacts

Helen Briant
Partner, Dispute Resolution and Litigation
☎ +44 (0)121 214 8867
✉ HBriant@trowers.com

Michelle Davis
Relationship Manager – Mid Corporates, Lloyds Bank
✉ Michelle.Davis@lloydsbanking.com

Dan Alderman
Relationship Manager – Mid Corporates, Lloyds Bank
✉ Dan.Alderman@lloydsbanking.com

Paul Latham
Client Development Executive – Gallagher
✉ Paul_Latham@ajg.com