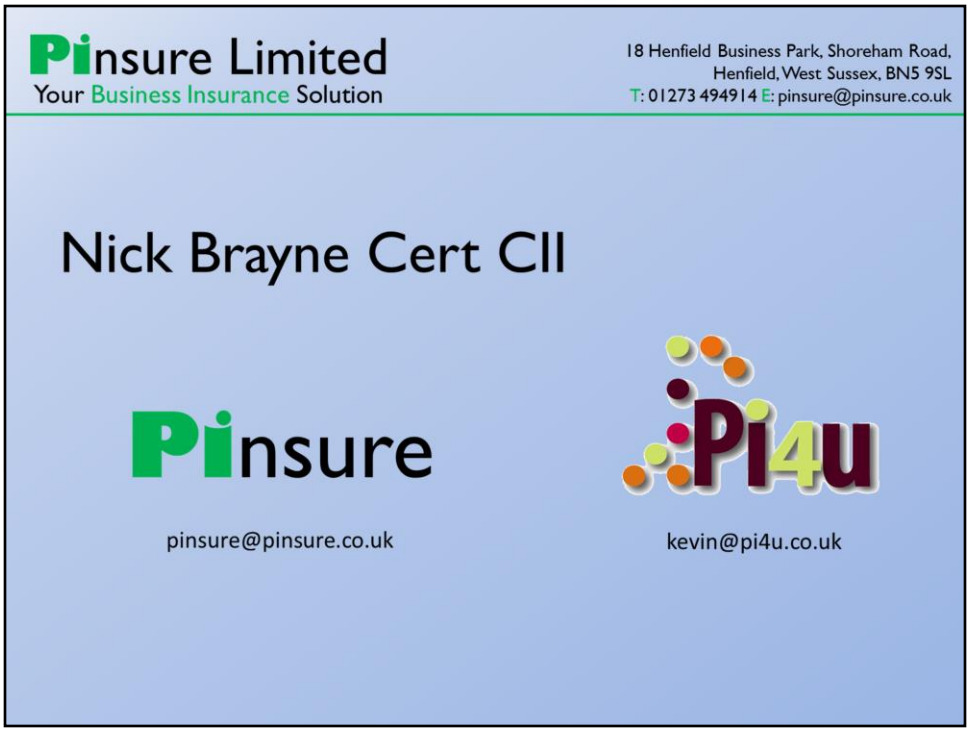
Pinsure Limited
Your Business Insurance Solution

18 Henfield Business Park, Shoreham Road,
Henfield, West Sussex, BN5 9SL
T: 01273 494914 E: pinsure@pinsure.co.uk

An Introduction to Cyber Liability Insurance



Nick initially worked in civil law, which provided an excellent background to his switch to commercial insurance in 2012.

Nick is now the account manager at Pinsure Limited, who are a retail insurance broker specialising in placing niche market commercial insurances such as professional indemnity insurance, directors' and officers' liability insurance and cyber liability insurance.

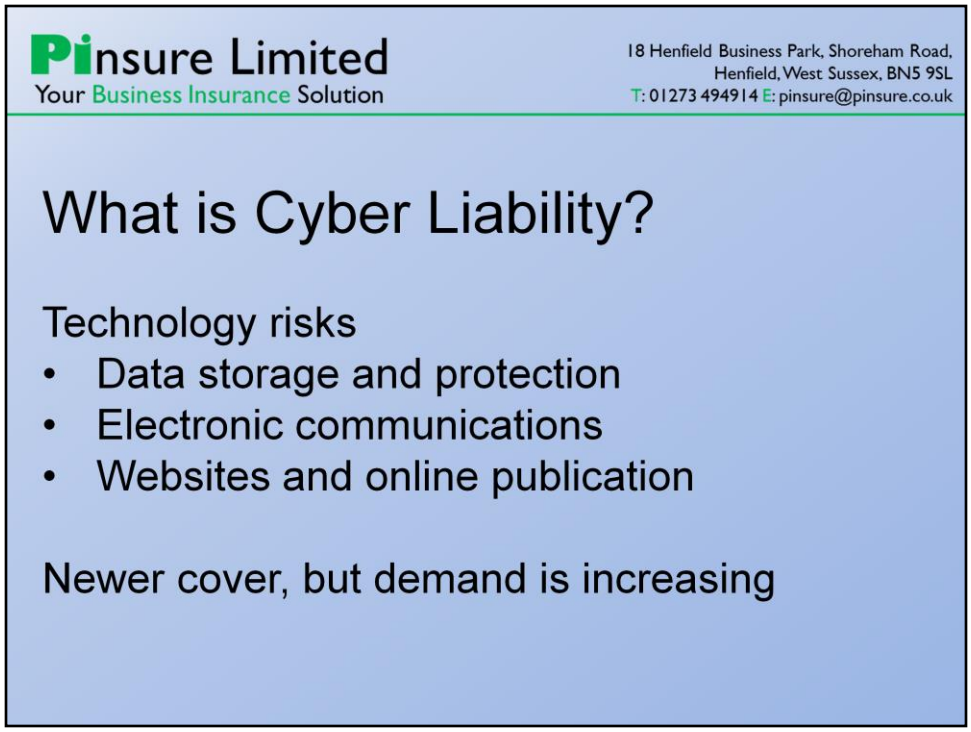
Pinsure Limited also has a sister company, Pi4u Limited. Pi4u was set up to arrange the same types of cover, but on a wholesale basis to their agents.

Pinsure Limited
Your Business Insurance Solution

18 Henfield Business Park, Shoreham Road,
Henfield, West Sussex, BN5 9SL
T: 01273 494914 E: pinsure@pinsure.co.uk

Learning Objectives

- The basics of Cyber Liability Insurance
- Common 1st party covers
- Common 3rd party covers
- Possible exclusions
- What client's say and common misconceptions
- How the law impacts Cyber cover

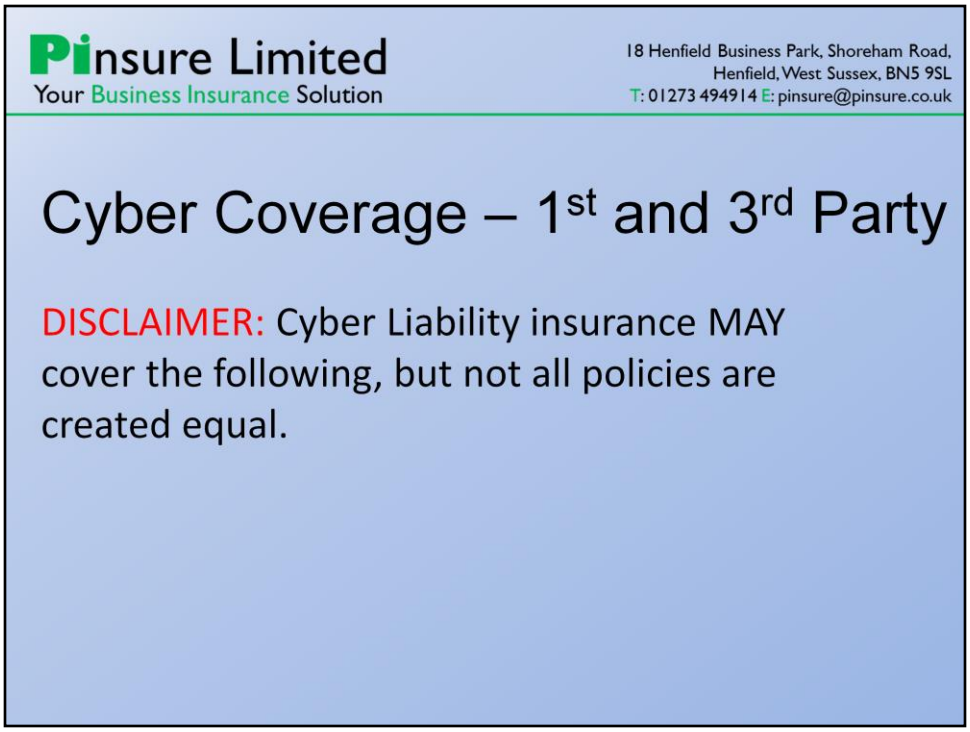


So basically, what is Cyber Liability Insurance?

Cyber Liability insurance provides a whole range of covers arising from technology risks. These risks could arise out of
•data you hold (e.g. databases, computer hard drives, e-mail accounts;
•data you transfer (usually by e-mail, but also audio or video streaming); or
•data you publish online (on your own website, 3rd party sites or social media)

Cyber Liability is still quite a new cover, however greater use of technology in all sectors, together with a number of high profile hacking cases, is leading to greater awareness of the risks and a greater demand for cover.

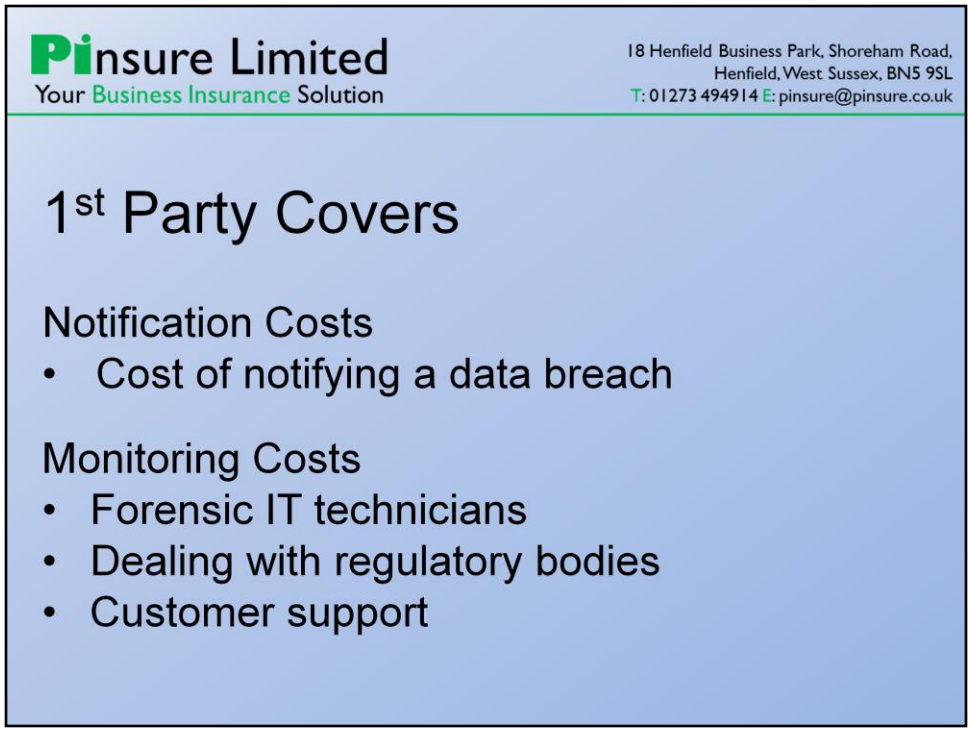
We also see a much higher demand for Cyber Liability in the USA due to their legislative requirements, which we will discuss at the end of this presentation.



Cyber Liability is a patchwork of 1st party covers (i.e. cover that indemnifies the insured directly) and 3rd party covers (i.e. cover that responds to claims made against the insured by 3rd parties). All of these covers will respond to various technology risks. I will talk about each cover in turn.

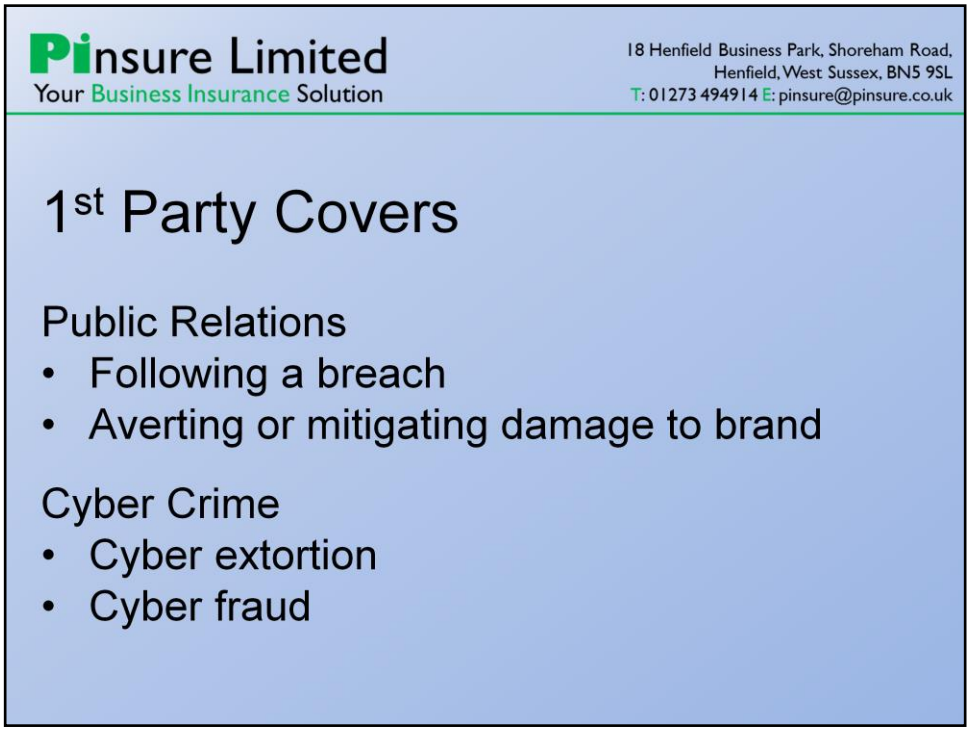
Disclaimer – there are a range of very different Cyber Liability products on the market. Some insurers will offer most or all of the covers discussed here, others are more targeted to a specific section of cover. A few insurers seem to have jumped on the cyber bandwagon without considering the full scope of cover required, and are currently offering very limited cover.

For this reason you should always check the policy wording to see what aspects are and are not covered. Remember that there is not yet a "standard" cyber liability policy wording.



Notification Costs
This covers you for the cost of notifying your client's that their data may have been compromised. The loss of data may arise from:
•physical loss (e.g. losing a laptop or phone);
•physical theft (e.g. a break in at you office to steal your server, or a backup drive being stolen from your car or home);
•hacker attack (i.e. someone hacking into your database, e-mail account etc. to steal data); or
•virus (whether this is a virus targeted at you specifically, or whether you simply fall foul of a general virus going round).

Monitoring Costs
This section offers other support covers following on from a data breach, and will usually include:
•forensic IT technicians to ascertain the reason for and extent of breach, and to stop the breach if it is still ongoing. These will usually be chosen by the insurer, and many insurers have their own specialist teams set up;
•Disclosing to and dealing with relevant authorities (such as data protection authorities); and
•Customer support costs, for example having notified your clients of a breach you may wish to have an incoming call centre set up to advise clients further

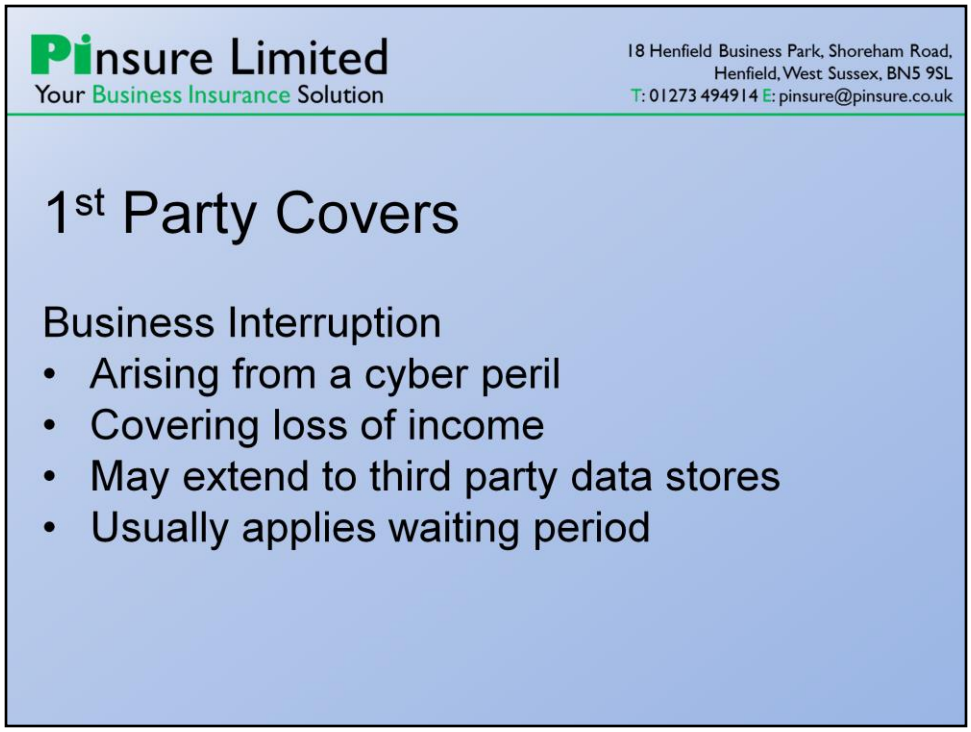


Public Relations
Having told your clients that you have lost their data, they may be somewhat unhappy. This section of the policy will therefore pay for the insurer's chosen PR firm to manage the effect a data breach may have on your reputation.

Cyber Crime
We usually talk about this as Cyber Extortion, and indeed some policies only specifically cover extortion under this section. This section of the policy will deal with technological extortion, such as:
•A threat of a hacking attack or a treat to release a virus if extortion monies are not paid.
•A virus locking down your system, followed by a demand for money in order to release the lockdown.
•A threat to release your client's data to the general public (where a hacker has already stolen this information) if extortion monies are not paid.

An example of this may be the Sony Pictures hack in November 2014, where hackers threatened to release unreleased Sony films which they had stolen, unless Sony agreed not to release the film "The Interview". As this is extortion for performance, and not directly for payment, it will depend very much on the policy wording as to whether a cyber liability policy would respond.

Some cyber liability policies will also respond to other cyber crime. The most common alternative example is cyber fraud. For example this could be a hacker putting their own bank details on your invoice template or payment system. It could also be a hacker stealing your client list and invoice template, and invoicing your clients themselves.



Business Interruption
This is a very valuable cover if written correctly. For this reason it is often not included as standard or at all, or only limited cover is offered.

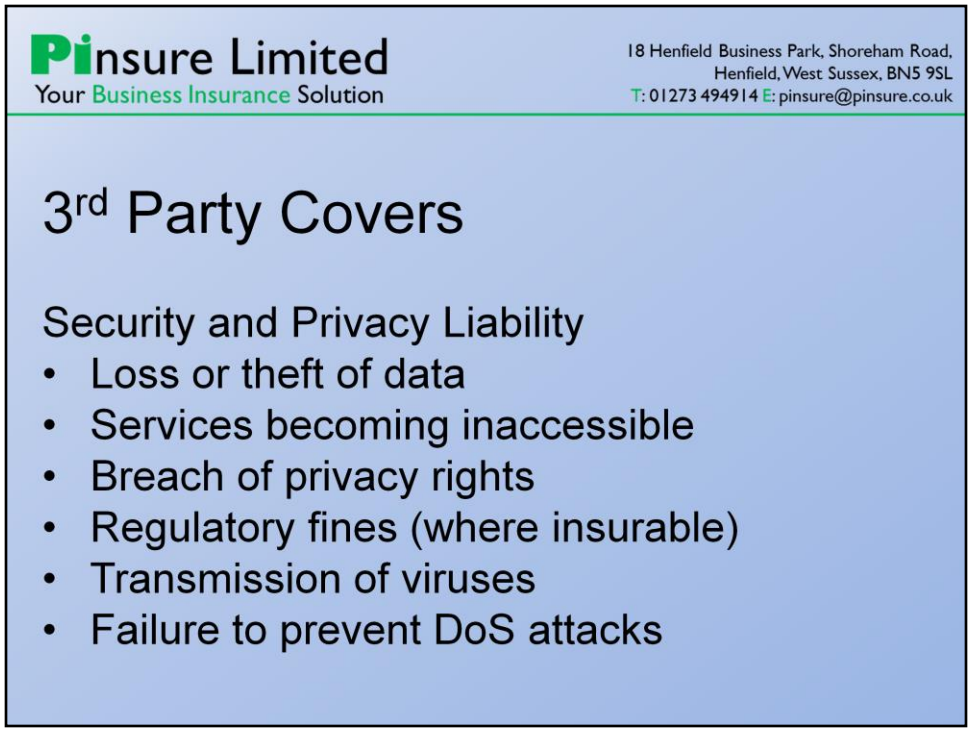
This is very much the same idea as business interruption cover on property policy, except that here the interruption must arise out of cyber peril. The policy will then respond to pay your loss of gross profit during the interruption period.

The definition of "cyber peril" will vary between policies. It should always include hacking attacks and viruses, where these lock your system or destroy data such that you are unable to trade.

Less commonly the definition of cyber peril may also extend to accidental damage (i.e. physical damage to hard drives or servers), and environmental factors (e.g. electromagnetic disturbances and solar flares).

A good cyber business interruption policy will also include cover where a cyber peril causes one of your suppliers to be unable to trade, and this causes knock-on business interruption to you. Here we are mainly talking about cloud storage companies or other third party servers that hold your data.

It is worth noting that usually cyber business interruption has a waiting period before policy will respond. This is often only 24-48 hours, and is to ensure that small issues are not notified unnecessarily.

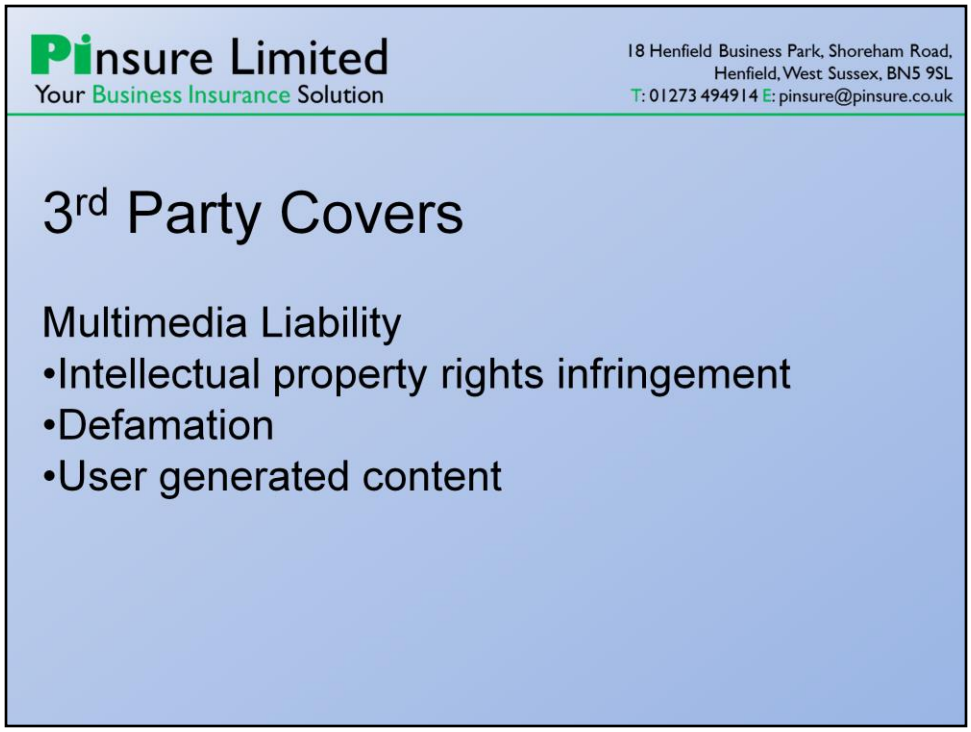


There are two main sections of 3rd party cover under a Cyber Liability policy.

Security and Privacy Liability
This covers a range of 3rd party claims which result from failure to adequately protect data or systems. Mainly these relate to loss of data as follows:
•It may be 3rd party has actual financial loss caused by you losing their data, or by their data being stolen and released to public. This is particularly obvious where confidential business information or trade secrets are held, but may also arise from loss of personal data such as account or card details. It may even be that loss of personally identifiable information results in identity theft, which then causes a 3rd party loss.
•A 3rd party could also have loss if they use services on your website (such as online trading and support services), and your online platform becomes unavailable due to a cyber event.
•A claim may be brought against you for breach of privacy regulations even if there is no direct financial loss, depending on the laws in the 3rd party's jurisdiction.
•In jurisdictions where government fines are insurable, the policy will also pay fines for loss of data. Please note that such fines would be uninsurable in the UK.

The other area that this section of cover will respond to is 3rd party claims due to your system transmitting a virus, or from being involved in a hacking attack such as a Denial of Service (DoS) attack. A DoS attack is where a computer or series of computers send excessive requests for information to a specific website, in order to cause the website to overload and shut down. These have been widely reported in relation to the hacker group "Anonymous".

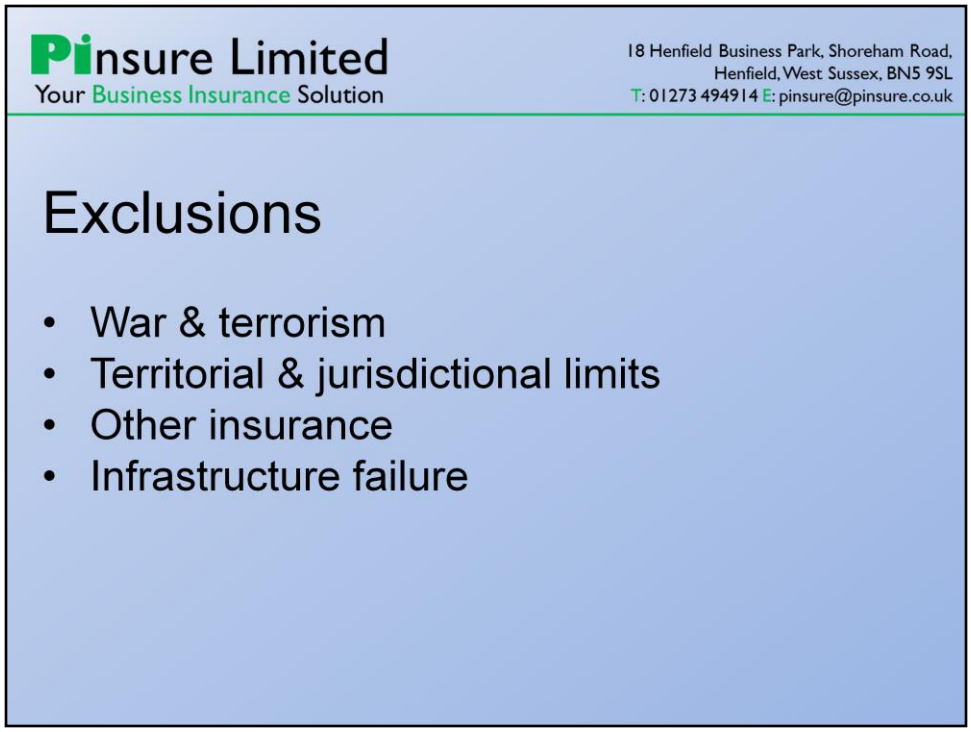
In both cases it may be that an employee is deliberately undertaking these activities on your network. More likely however is that your network is hacked or receives a virus, which then takes over your network to undertake this activity. This can occur without your knowledge that there has been a breach, however you still may be liable to a 3rd party for the activity.



Multimedia Liability
This is the other main 3rd party cover under a Cyber Liability policy, and covers 3rd party claims arising out of the information that you publish and transmit online. This could be content published on your own website or on a 3rd party's website, including social media, or may be content transferred in electronic communications such as e-mail.

A claim here may come from alleged infringement of intellectual property rights, such as if your logos or images infringe on a copyright, or if the content on your website is plagiarised from another source. You may also receive claims for defamation (libel) should a 3rd party allege that your website or e-mails contain defamatory statements.

The above covers may also extend to include user generated content. User generated content would include anything written on a message board, forum, comments section or rate and review section of your website by a member of the general public. It is important to cover this content as, whilst you may not have created the content, you may still be found liable for hosting material provided by others as you may be deemed to be a publisher of this content. It is for this reason that websites such as YouTube comply so stringently with demands for material to be removed, as they may otherwise be found guilty of publishing copywrited material submitted by a third party.

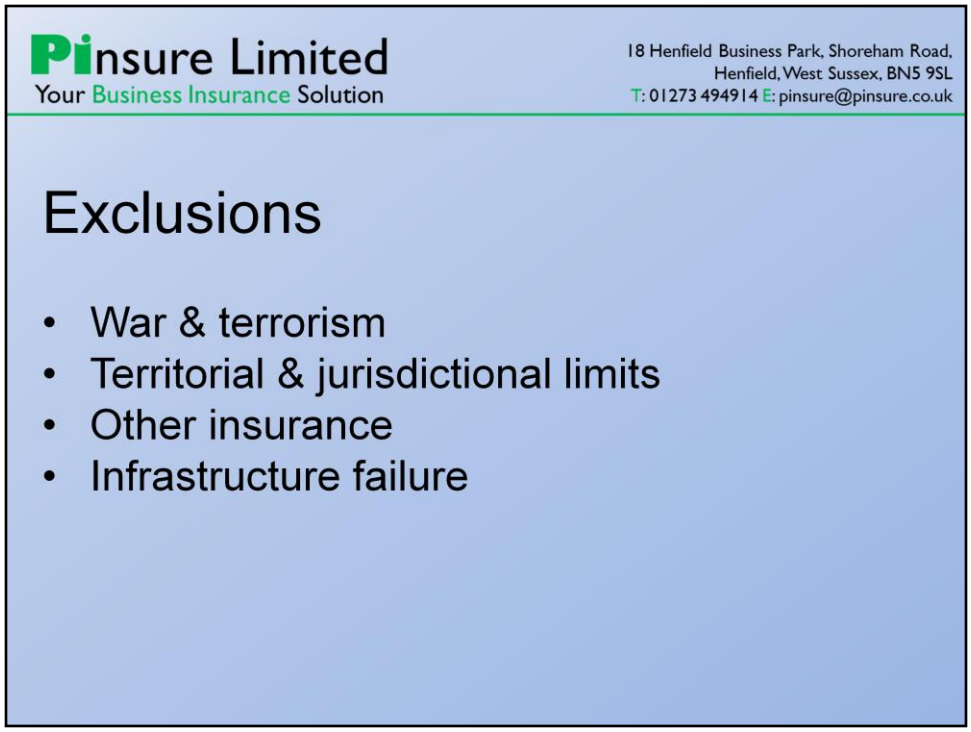


Now we are going to move on talk about exclusions. The exclusions listed here are not necessarily common exclusions, but rather are ones to be aware of.

War and Terrorism
As with most policies there may be a war and terrorism exclusion on a cyber policy, and in itself this is not a problem. However, you would need to ascertain whether this exclusion only applies to physical acts of war and terrorism, or if it can be interpreted more widely.

In its widest interpretation terrorism could include hactivism, as we have seen in the last few years with hacktivist groups such as Anonymous, Lulzsec and Lizard Squad. The definition of War could also be implied to include a hacking attack by a foreign government in a war situation. This scenario could certainly arise if the insured has contracts with government of military bodies, or if they are perceived to be important to the country's infrastructure.

A few insurers make clear in the policy whether the above examples are intended to be excluded. If the is a war and terrorism exclusion on the policy without further clarification you should check with the insurer whether this extends to hacking as part of war or terrorism.

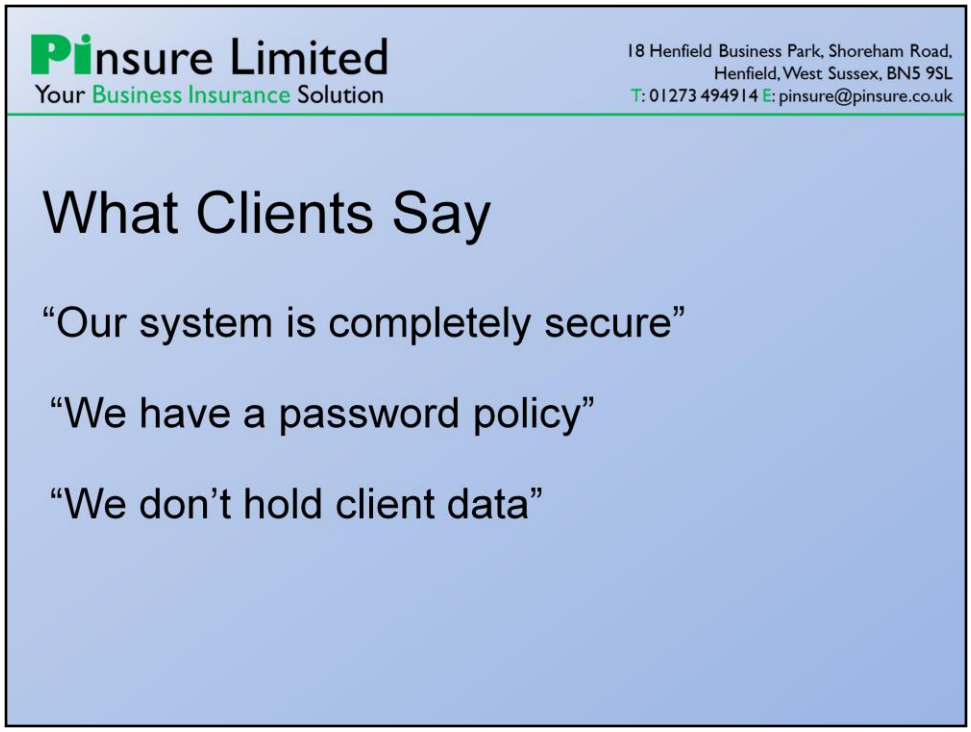


Territorial and Jurisdictional limits
Put simply, these should never appear on a Cyber Liability policy, as Cyber Liability is by its very nature worldwide. Regardless of where the insured and their clients are located, anything online can be accessed anywhere in the world, and a claim could come from anywhere where your content can be accessed.

In addition, if your cyber business interruption will respond to interruption at a cloud storage company, which turns out to be located in an excluded territory, then this will no longer be covered. It is particularly worth noting that a large number of cloud storage warehouses are based in Canada, which is often seen on these exclusions.

Other insurance
As with most policies, you may well see an other insurance exclusion on a Cyber Liability policy. It is therefore worth mentioning that there may be some overlap between Cyber Liability and other policies. In particular 3rd party covers, such as intellectual property infringement and defamation, may also be found on a professional indemnity policy. We are also now seeing a few standard business interruption policies extending to cover cyber business interruption. This is simply something to watch out for, and if possible it will often be best to place the Cyber Liability with the same insurer as the professional indemnity insurance to avoid any conflict.

Infrastructure Failure
This is a common exclusion on Cyber Liability policies, which excludes claims relating to failure of necessary infrastructure (which will likely be either an electricity or internet outage). From insurers' point of view this is a very sensible exclusion to stop catastrophe claims from large outages. Please therefore note that this exclusion will likely be in place.

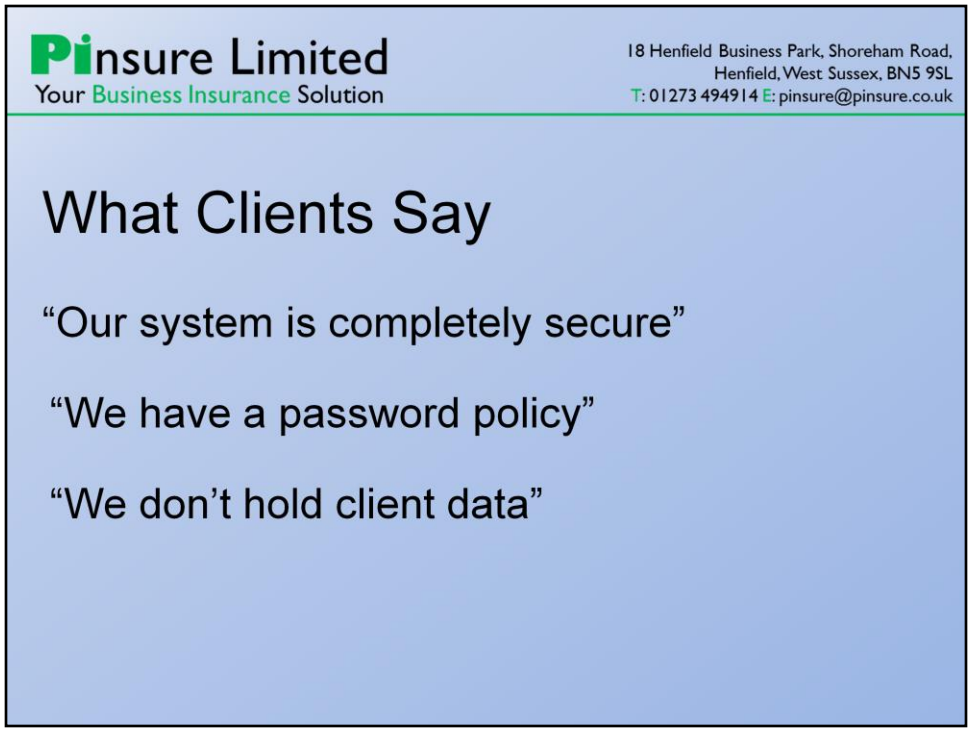


Now I will briefly go through a few things clients commonly say when offered Cyber Liability policies.

"Our system is completely secure"
You will hear this a lot, especially where the client has a chance to speak to their IT consultant before coming back to you. IT consultants don't generally like to admit any insecurity in a network as they are of course paid to minimise this risk.

No system can be completely secure however. In the past weeks we have seen TalkTalk hacked by a lone 16 year-old. Last Christmas both Microsoft Xbox Live and Sony PlayStation Network were hacked. If these major technology companies with huge cyber security budgets can fall victim to hackers then anyone can.

Even if a database is not connected to the internet at all a server or hard drive can still be physically stolen from an office and subsequently accessed.

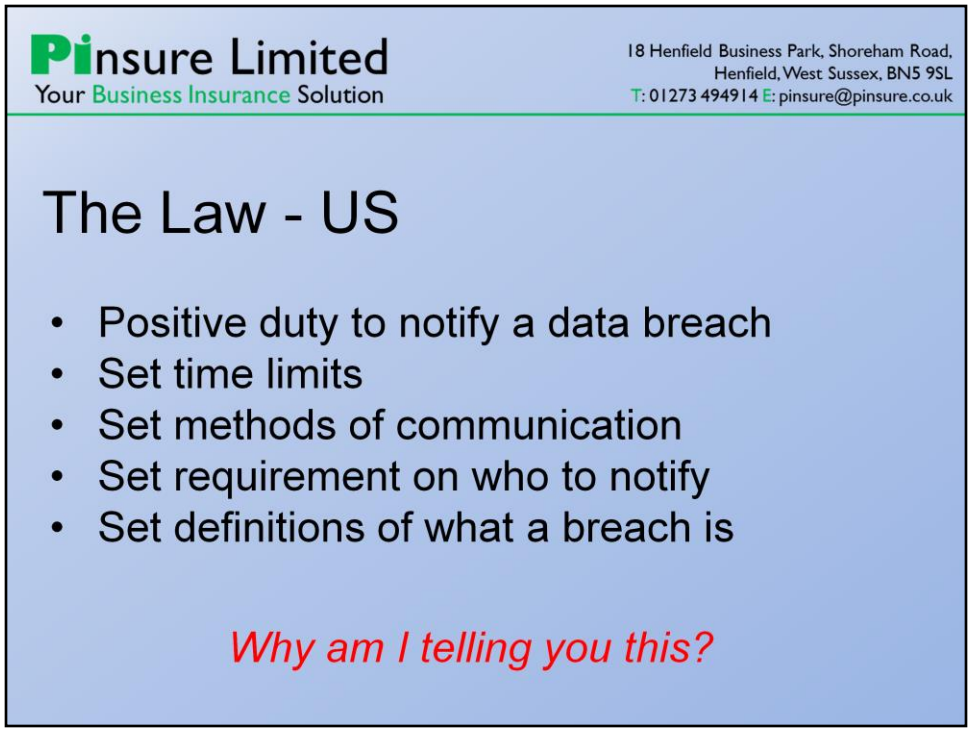


"We have a password policy"
Some clients will believe that a login password is all they require to protect their system. Unfortunately no password completely secure. One system of password cracking, known as the brute force method, involves a computer simply guessing every possible combination of characters until it gets through. This may sound like a long process, but a 6 character password can still be cracked in just a few minutes.

Longer password are better, and using symbols, capital letters and numbers is good, but it is still not a case of *if* a computer can break the password, it is simply a question of *how long it will take*.

If the hacker can get hold of physical hard drive the process is even easier. If you take a hard drive and connect it to a separate computer then you will not need a password, as you do not have to go through the boot/login process. If the data on the drive is unencrypted you can then view all of the stored information without a password.

"We don't hold client data"
Some clients (although usually not in office based professions) may not feel they have any client data to lose, as they do not maintain a large database. It is important to point out to these clients that it is not just a central database than can be hacked. If the client ever communicates with their clients by e-mail then this information can potentially be lost or stolen, and this client information needs the same level of protection that an in-house database does.



Finally we will briefly talk about the law relating to data breaches, starting with American legislation.

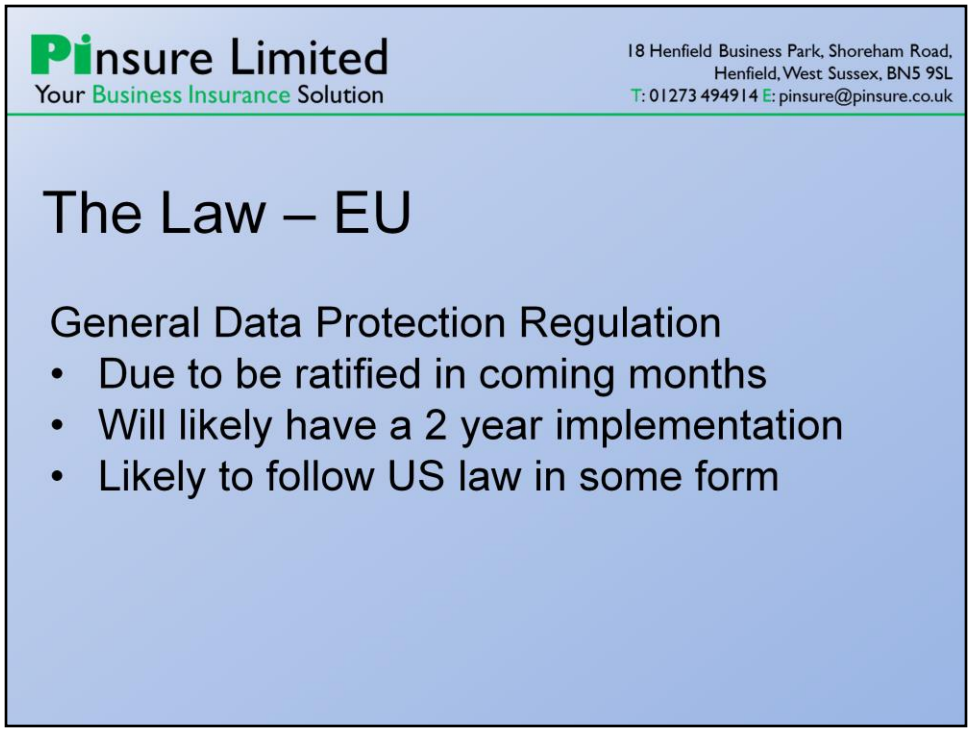
There is state level law in most US states relating to breaches of third party data. President Obama recently announced an intention to introduce federal law to codify the requirements of the various state laws on this subject, however they currently remain seperate. In all cases this will impose a positive duty to notify your clients of a data breach, with various penalties for non-compliance. You can therefore see that the data notification costs we talked about earlier suddenly become extremely important.

Beyond the above duty, the requirements of the law vary widely between states. Firstly there will be a set time limit to notify clients, which could range from as little as 24 hours to as long as 28 days.

There will also be various methods of communication required, and various requirements on who to notify. For example you may be required to notify all of your clients that their data may be compromised, or only specific clients who have had data compromised, or only specific clients who have had certain types of information compromised (brought about by different definitions of the term data breach).

But we're not in America, so why am I telling you this? Firstly, it's worth noting that law applies where the end client is, not where you are based. Therefore a UK company with US clients would need to comply with the relevant US legislation.

Secondly...



Secondly there is new legislation going through European parliament at present, known as the General Data Protection Regulation, which will impose a similar positive duty to notify third parties of a data breach.

This has been long process, having started in 2012, with various politicians and firms lobbying for certain requirements to be incorporated in to the legislation. There has also been a big American influence on the process, with US companies and politicians looking for laws no more restrictive than their own domestic laws.

In theory this law is due to be ratified this year, although we may not actually see this until 2016. As the draft legislation is currently drawn member states will then have a two-year implementation period to bring this into their own laws. We will therefore be looking at this coming into force in late 2017 or early 2018.

As this legislation is still in draft form it is not possible to discuss what it will contain in detail. One requirement in the current draft is to notify relevant authorities of a breach within 72 hours of the breach. Notification time for contacting clients is as yet unknown.

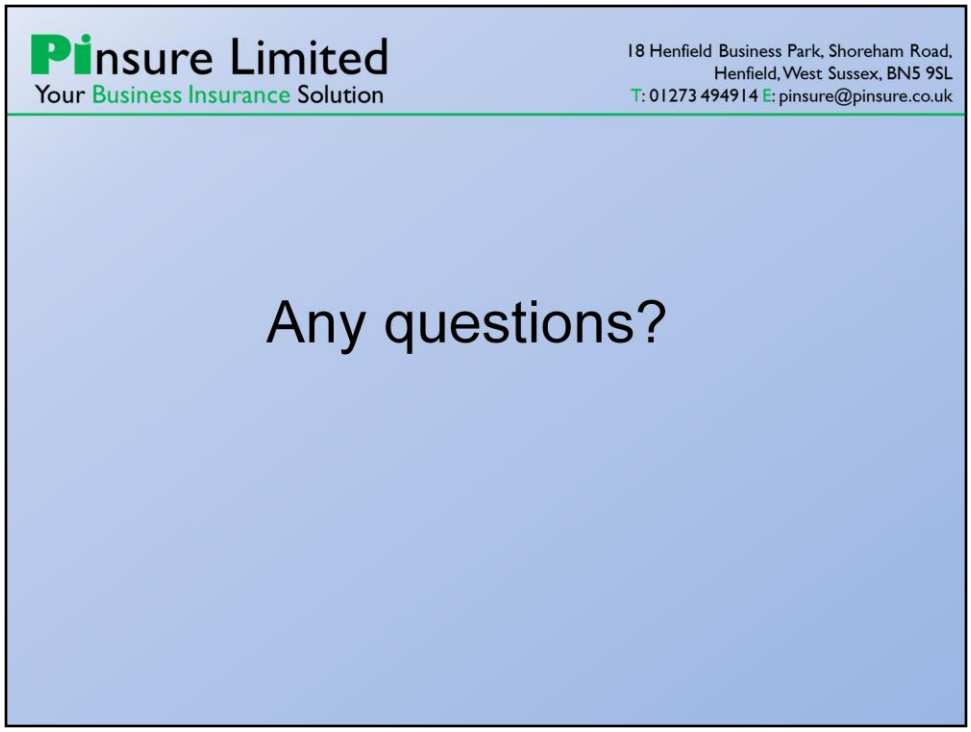
When this law come in, it will turn cyber liability from being a useful policy that is good to hold into an absolute requirement for most companies.

Pinsure Limited
Your Business Insurance Solution

18 Henfield Business Park, Shoreham Road,
Henfield, West Sussex, BN5 9SL
T: 01273 494914 E: pinsure@pinsure.co.uk

Learning Objectives

- The basics of Cyber Liability Insurance
- Common 1st party covers
- Common 3rd party covers
- Possible exclusions
- What client's say and common misconceptions
- How the law impacts Cyber cover



If you have any questions on the topics contained herein, or if you require a quotation for your own cyber liability insurance, please contact me on 01273 494914, or by e-mail at nick@pinsure.co.uk.

If you are looking for quotations for your clients' cyber liability insurance, please contact my colleague Kevin Locke of Pi4u on 01273 494914, or by e-mail at kevin@pi4u.co.uk.