By Darren Vye, Cyber Lead & Professional Liability Claims Manager, Vice President - at Arch Insurance

And David Clarke FBCS CITP, CTO The TrustBridge

Edited by Penny Heyes, COO, The TrustBridge

As we see an increase in the number of cyber attacks and ransomware incidents, we are examining whether Cyber Insurance is fit for purpose: is it worth it? Will it pay out? How the insurer actually responds to security incidents, what are the risk elements and how to mitigate those.

Cyber insurance has changed quite a lot over the years. From being cyber liability insurance, which basically covered the third party claim, it has evolved to include the first party claim. The focus is effectively to get the insured's (the client) operation back up and running and in the same position as it was prior to the incident. The claim will include all first party costs such as defence costs, legal cost, expertise costs, forensic accountants, public relations costs. All this falls under first party claims.

Some insurance policies will cover the business interruption element too, but not all policies cover this.

In the event that the insured's (the client) operation is disrupted, or even ceased, for a number of days, there are policies that can reimburse the insured for any losses arising from the time when it is not operational. That can be quite a long time.

Liability can cover the first party and third party and sometimes it may well pay the ransom.

Ransomware attacks

There are many dos or don'ts in terms of ransomware payment; whether you pay the ransom, whether you don't pay the ransom, what is the impact on restoring the operation post ransom? Will the insurance policy cover the ransom payment ?

If you are a business owner or senior manager of an organization, you will want that company or that organization back up and running as quickly as possible, and you're managing this situation under tremendous stress.

The immediate response is to pay that ransom, but actually there are consequences for paying, including potential criminal proceedings. If you have paid that ransom to known criminals or to a terrorist bank account, then you could be liable for a number of charges and fines.

So it is key to exhaust all avenues before paying; forensic experts can ascertain if backups are working, or whether the insured is going to be affected and in-operational for months or not. The client will always want the quickest solution, but they should not make any rash decisions to pay the ransom where maybe they don't need to.

The insurance company employs experts who will go through a due diligence process in as much detail as possible before making any ransom payment. This due diligence will include making sure

that the ransom demand is not coming from anyone on any criminal list, that they are not on any terrorist list. So there needs to be a sanctions check when making that kind of payment.

Insurance companies are very, very careful and will only pay a ransom as the last resort. However, it is not a case over just handing over the money and trust that the attackers are going to honour the deal. The insurer has to ensure and prove who the attackers are and prove that they have got the decryption key to release the data, prove that they've got the evidence. Insurers like to get a "taster" to make sure that the attackers are really going to surrender the key and that the key will work.

There is , surprisingly, a code of conduct between Cyber criminals that they honour the ransom payment -i.e. that if they demand a ransom to get the organisation back up and running, and then once the ransom is paid, that they don't demand a further payment. This code of conduct amongst criminals ensures that, if they do renege on the deal, they would get a known reputation within the expert world. These experts are advising both insurers and the clients and will know if the key is likely is to be supplied on payment of the ransom, or if the client is wasting money. If the insurance pays the ransom or negotiates the ransom, the client's backup can be re-reinstalled and the organisation can be back up and running within a few days.

It is important to secure that exfiltrated data has not been sold on – which would cause an almost bever ending issue. Although difficult to safeguard against that, as part of the negotiation of the ransom it is important to suppress the risk that the attackers distribute your data.

On the basis that the data could be destroyed, it depends how valuable that data is, so the insurance company needs to evaluate their response very carefully.

The best end result is always to get the client back up and running as quickly as possible.

Negotiation

The insurer will work with the client to retain all the relevant experts such as intermediary negotiators, forensics, PR consultants etc. Negotiation is very technical, so insurers do not generally get involved. The negotiators are normally embedded within the IT forensics or there are independent companies who can help. These negotiators tend to know all the criminal groups, they keep records of who they are paying and who they are negotiating with. They learn to recognise their traits and how they communicate such as the language, the spelling errors, the grammar they use. Having studied this, these negotiators know whether or not these people are genuine or part of a nefarious criminal gang.

Risk Assessment.

When underwriting a risk, the insurer's underwriting team will undertake a full due diligence on every client before they take out insurance. Many insurers offer a key service – pre-breach assistance to review the current incident plan, asses the risk and to train personnel.

This process would include a scan of their systems to make sure there are no vulnerabilities to ensure the client is a better risk and can avoid a data breach. Some clients are uncomfortable with this process, believing that they don't need it. However, the more breaches and security incidents occur, the more clients are approaching insurance companies to take our cyber insurance.

In fact, there are some new rules and regulations surrounding the training, the preparation and the testing that has to be done now with organizations around data and cyber incident and the plans they have on place.

Reducing the insurance premiums

A company can help itself become a better risk by undertaking certification such as the UK government's Cyber Essentials Programme or ISO 27001, and develop a WISP (A Written Information Secuity Programme) and this will help it survive the insurance company's due diligence and can substantially reduce the premium.

Through indepth preparation prior to any breach happening, a client reduces the risk of any potential incident. This is attractive to an insurer because if, if the client is a better risk, the risk is lower for the insurer to take on.

The reponse

Once insured, and in the event of a security incident, the client organisation will know the first port of call, they can pick up the phone and speak to their insurer before taking any action and not instigate any action themselves. This ensure a greater level of control for the insurer who is there to help from the start and is fully engaged with the situation, rather than coming in a later date which could affect the likelihood of a payout. If involved from the beginning of an incident the insurer can provide the client whatever assistance they need, whichever vendor or expert they need. A swe have stated, it is in the insurer's interest to get the insured back up and running as quickly as possible.

Within the attacked organisation it is key to ensure everyone knows the escalation process? Who's managing the social media feed? Who's managing communications out to the wider world, to the public, and to the people that have been affected.

Non payout

Are they any key situations where insurance would not pay out, key errors that companies make, which would invalidate their insurance?

If a client dealt with the cyber loss on their own, paid a ransom and dealt with the situation, got themselves back up and running but then reported the incident to the insurers, some weeks / months later to make a claim, this would make the situation more complex in terms of reimbursement as the insurer would not have been involved. Many policies require that an incident needs to be reported immediately. So, the insured has a duty to report it to insurers and get the authority before they retain any experts or have any negotiations or pay any ransom or incur expenses.

Cyber insurance policies are there help and respond to an incident, every step of the way and the client would get guidance and information from the insurer to deal with the situation.

Fines

Potentially, there are fines associated with any data or cyber breach, especially if there is any issue with the data subjects who may have suffered id theft, financial loss or personal reputation loss.
If an organisation is prepared and has data breach plan in place and can show (evidence) that they have done as much as it can to mitigate the risk of a data breach, and is seen to be doing the best it

can with the resources it has and the capability it has, appropriate to the size of the company, it can minimize those fines.

A fine from the regulatory authority is unlikely to be recoverable under insurance policies. The insurer would obviously work with a client in terms of trying to minimize the risk of any fine but it would be the view of the regulator that the fines are for the organisation, not for someone else to pay.

Back ups and Recovery

If an organisation has a back up system, it is likely to be in a stronger position (potentially) whilst undertaking any ransom negotiation. If you are able to get back up and running, then you are negotiating on how the data will be used, has it been exfiltrated, will it be spread all over social media, sold on the dark web etc. This is an easier negotiation in theory, than if your business is in-operational and you are negotiating for the organisation's future.

If your systems and data are "returned", it may be that they are no longer in the same state that they were because they were infiltrated. The system need to be upgraded and protected to make sure an attack won't happen again a week or a couple of days later.

Even with back up systems and data, it can, unfortunately, take a while to restore it in an unacceptable time frame . Often there is a rebuild of systems required – all this contributes to lack of business continuity, and loss.

3rd party loss

If a data subject has suffered a personal financial loss, for example, as a result of a data breach, would cyber insurance cover this?

Where a third party data subject has suffered as a result of a cyber event and they claim against the client this would trigger a standard cyber policy claim. This could be quite substantial if, for example, a class action suit was taken out.

Such claims would come under third party liability which would be triggered by the policy. Obviously, the loss would have to be proved to be related to this case. If we know that there has been a data breach and individuals' data has been made available on the dark web or used, the insurer will advise the client that it would pay for (e.g) a year's credit monitoring - a bit like another insurance policy for that individual. If there is any activity using that individual's data, such a credit card being applied or their name being used in a loan, this will be flagged for the individual to approve. Some insurance companies are providing three years credit monitoring, but this is not universal.

If an organisation is in a 3rd party supply chain in which a cyber incident has occurred – that is not their fault but they have suffered as a result, whose insurance policy pays out work in that situation?

Normally it would be expected that the third party's insurance company would pay out, therefore it is key when undertaking due diligence (often with questionnaires) that your 3rd party suppliers have their own insurance in place. However, whether an attack arises from a third party or not, your insurer will help, retain experts to manage the fall out. It is likely however that, after the event, the insurance company will be looking to that third party for a recovery of costs.

So it is key when answering such questionnaires, or reviewing any 3rd party's WISP that a client raise any issues regarding insurance.

The right policy

Insurance companies work with their clients when putting a policy together to try and find the right policy for them. The client should prepare and then work with the insurer in a pre-breach assessment to ensure any holes and gaps in their data protection and security protocols are filled. Training is a key part of this process.

If clients really embrace cyber insurance and believe that they want and need it – they are more likely to make sure their systems are tight and be happy to undertake this pre breach assessment.

Summary

So as with many data protection and cyber security protocols, the key question is how do you mitigate and minimize the risk of a data breach?

- Follow best practice and government guidance.
- Staff training is key.
- Make sure the company's senior management and staff are all fully on board with the right policies and procedures, and that they are well understood within the company.
- Undertake internal audits, external audit, and due diligence on any 3rd party.
- Have multiple layers of security and make sure those multiple layers work.