Insure for Cyber Security

Jason Cobine, Managing Director of Cobine Carmelson, protecting Assets, Income and Reputations, discusses how best to insure for Cyber Security.

Cobine Carmelson Ltd
Not just insurance - Reassurance

Before we get started, let's deal with the issue of paying a ransom if hackers get in. I have seen the articles stating that hackers will target companies that have insurance that pays ransom demands. The "risk management" advice was to make sure that your insurance documents were well hidden, so they couldn't hack in and find them. Other advice was not to buy insurance that pays ransoms.

Yet what if the cyber thieves had access to insurance company databases? What if they divided them into those that do and those that don't have cyber insurance? What if one gang targeted those with insurance and another targeted those without it?

Hiding your documents wouldn't work. Not buying the insurance makes you less resilient if you are caught up in an attack. Not only do you not have cover for ransom, you don't get access to the experts in such negotiations which is vital. It will be the organisation paying the ransom. The insurance policies pay it back to the organisation.

Do not make the mistake of thinking that insurance companies treat their employees so well that they would never imagine stealing data. It is quite the opposite. There are court cases every day about employees being poached. It would be naïve to think they don't take data with them. If a "bad leaver" can access the data, "bad actors" can too.

So if an insurance company has a problem with data security, make sure it remains their problem. Don't pay too much attention to those that come up with reasons why you shouldn't buy insurance for ransoms. Or at least think about their motivation for making such statements.

Taking the moral high ground could prove to be an expensive mistake.

Assess the risk! Yet make sure your risk assessment covers the intangibles such as intellectual property and culture.

Keep in mind that France has banned the sale of insurance that pays ransoms, so we'll keep an eye on them and see how it pans out. If it works out well, we can all stop buying insurance for ransoms.

CISOs Under Pressure

At a recent conference for CISOs (Chief Information Security Officers) it became clear that there is a conflict between IT/data security and insurance. Over the last few years, CISOs have found it increasingly difficult to carry out their role.

CISOs do their absolute best to make sure the IT is secure, and then insurance companies dictate standards that are unnecessary and, in some cases, make no sense.

Yet insurers still insist that the organisation must meet these standards. The fact that these standards may have been built by banks or other sectors is lost on the underwriters.

There are even cases where companies have received 60 page questionnaires from insurers, such antics act as a barrier to doing business together, it certainly does not remove friction.

So how can the road be smoothed and gaps between IT security and insurance be narrowed?

Insurance companies will listen, if they are motivated to do so. IT teams and CISOs will make better decisions about insurance if they think insurers are listening and making sense. The underwriters at insurers must be motivated to listen. They do that when they see profitable opportunities. What they often feel is "I'll get sacked if this one goes wrong".

Insurance must be seen as a last resort. The fact that insurers provide services in the event of a digital interruption, rather than purely cash, shows that cash is often useless without support.

A risk assessment will determine what is most important, yet don't forget the intangibles. For example, a lot of risk assessments end up requiring "more security" or "more insurance" yet they are 4th and 2nd on the list of methods of reducing risk. There are other ways of reducing risk and they must be investigated.

The risk that will cost you the most is the one to concentrate on. Why are your most valuable assets not in the safest place that you know about? When you're at home, you don't leave cash, devices or other forms of currency in the open?

> ***"Taking the moral high ground could prove to be an expensive mistake"***

The relationship has to be built with bridges of trust and grey areas have to be made black and white. You can do that by highlighting risks (instead of hiding them) and reflecting what you have done about it.

If you did all you could to reduce risk and presented that clearly, an underwriter would give you a better deal.

When you assess the risks to your organisation, it cannot be too generic so don't forget the intangibles. Work out which ones you can cope with, insure the unmanageable and accept an excess on your insurance. An underwriter will love it if you're sharing the risk with them voluntarily.

Where do we Draw the Line?

Never an easy thing to decide, yet you should only insure the things that you can't afford and definitely not be trying to cover the things that you can.

If you can't move it to the safest place on the planet, can you move it to somewhere safer than it is?

You can't 100% stop people getting in, yet you can make it more difficult. Please don't "bury" your back up. You might need it. Insurers preference is that you have a backup that is kept nowhere near your systems. Yet it must be accessible and retrievable, I've lost count of the amount of untested backups

The Culture of Risk

If people don't use the controls, is adding more going to work? Or do the people need more encouragement to take action?

Before you add controls, you really should find out why the existing controls are not being used. And please listen. Don't behave like Insurance companies, they ask us for feedback daily yet they never, ever seem to act upon it.

Have you asked your marketing department to get involved in your data security communications? People do need strong messaging and reinforcement yet that must be tested and measured. Like all your marketing activities. Test and measure your messaging before adding more layers.

We need to stop applying more rules to those that are not working. IT security can go unused or switched off if staff are "unengaged". Getting the culture right is so very important.

Keep in mind, no matter what level of security and insurance is in place, we do leave our assets exposed if our company culture is not right. Organisations waste a lot of money on security and insurance when it is their culture that has to change. There are tools to assess this risk too.

About the author:
Jason Cobine

Jason Cobine is an Insurance Broker working with Managing Directors, Partners, Business Owners and Founders who are not 100% certain they have the right cover for claims they want to make (or defend). For more than 25 years Jason has been helping organisations mitigate exposure of their assets, income streams and reputations, in essence, protecting their organisation against the unthinkable.

Scan the QR Code