


Unsure on insurance

With the insurance industry boasting of rapid increases in cyber insurance business, should the channel be more open to the idea, or batten down the hatches, asks Tom Wright?



Tom Wright

 @TomWrightCRN

16 January 2017

You expect the vast majority of households in the UK to have failsafes in place to help to prevent burglary.

Presumably all doors and windows are fitted with suitable locks. Then perhaps, if these fail, there is a burglar alarm to alert neighbours and the police. In the unfortunate event where these both fail and prevention is not possible, there is a lifeline - the insurance policy that you have been paying for the last 20 years in anticipation of maybe using it one day.

If paying to insure your physical possessions is second nature to homeowners, why is the concept of insuring your virtual possessions not so common?

Channel reluctance

The concept of cyber insurance isn't an especially new one but it is relatively unexplored, particularly in the UK.

The channel has never really been a fan - as shown in the CRN Online Security Summit in 2015 when it was branded "not worth the paper it is written on".

Cyber insurers themselves, however, will point to rapid growth in the number of policies taken out in recent years as an indication that end users are coming around to the notion.

A report published by Allied Market Research at the end of last year predicted that the cyber insurance market will be worth \$14bn (£ 11.3bn) globally by 2022 - nearly five times the current estimated market value of \$3bn.

Meanwhile, the fines set to come along with GDPR (General Data Protection Regulation) spell out what, cyber insurers claim, is shocking businesses into action as they fear paying out up to four per cent of their annual revenue if they are found to be negligent.

London-based CFC Underwriting has been in the cyber insurance game for nearly 16 years, but Graeme Newman, the firm's chief innovation officer, admits that the UK has not so far contributed much to business.

"If you look at cyber insurance in the UK compared with the rest of the world it is interesting because the market itself is very US dominated," he said.

"If you look globally, 90 per cent of all cyber insurance that is written is for US companies.

"Twenty-five per cent of businesses in the US buy cyber insurance, but by contrast less than five per cent of UK businesses would buy specific standalone cyber insurance. It's a big contrast and it raises the question of why, because in many respects there shouldn't be any difference."

Newman explained that US uptake of cyber insurance stems from highly publicised security breaches over recent years, coupled with the fact that American firms have been obliged to

disclose information regarding privacy breaches for the last 12 years - heightening fears of damaged reputations among businesses.

These types of breaches have started to creep over the Atlantic - the TalkTalk hack being the most noticeable recent example - while ransomware attacks on SMBs have increased rapidly.

Newman said that these attacks, along with increased awareness of cyber insurance at security summits, means UK businesses are becoming curious about the benefits of a cyber insurance policy. CFC saw its own UK cyber insurance business double in 2016.

The IT industry, however, is still reluctant to accept cyber insurance, he said.

Fear of the unknown

"There has been a real - I don't know if it's a mistrust, or a misunderstanding or a fear - from within the IT security industry that somehow insurance is going to replace what they do," he said. "It's a really odd strand of thought and it comes from ignorance, in the nicest possible way.

"It's a lack of knowledge about what this is because insurance does tend to disrupt existing markets.

"The first home insurance policies were created a couple of hundred years ago and now it's at a tipping point where insurers have started to dictate the locks on the doors and the types of alarm used. That happens over a period of time and there is a nervousness within the IT security industry that it could be starting to happen there - so in essence they might want to stop the growth of insurance."

Newman explained that some in the IT security industry are under the impression that spending on cyber insurance will take money out of the budget for security spending, when in fact it is most often the opposite because insurance packages can act as a financial vehicle to pay for security services.

"It's just absurd," he said. "It would be like saying 'I don't think I'm going to bother with any sprinklers or alarms in our building because we're just going to buy insurance instead!'"

While Newman laughed off the notion that cyber insurance will eat away at IT security budgets, Carl Gottlieb, founder of security reseller Cognition, said smaller businesses with tighter budgets would face an either/or choice.

"The growth in cyber insurance is much more rapid than the growth in product sales," he said. "It estimated that in the next few years there's going to be a greater budget spent on insurance than actual prevention, so you have to ask where is the money coming from for insurance? It's got to come from somewhere and ultimately it could be the same security budget.

"There will be a shift away from prevention to insurance, and that's not what anyone wants to see especially with GDPR, which is all about protecting your data, not waiting for it to be breached."

Will they pay out?

Gottlieb claimed that the primary concern around cyber insurance for Cognition's clients is reluctance from the insurance company to pay out in the event of a breach. He said that, more often than not, insurance companies will try to prove negligence on the end-user's part, meaning their claim is invalid.

"If I break into your house because you don't have a 30-foot steel gate outside it, is that your fault?" he said.

"The question is 'are people liable? Are they negligent?' That's a really difficult thing to prove, but some of our customers have looked at these policies before buying them and said 'we don't think you're going to pay out'.

"It's very tough for end users to know what to do with that so at the moment all we're telling end users is to prioritise their spending on reducing the risk and preventing data breaches."

Role of the channel

While all the signs point to an increasing uptake of cyber insurance whether the channel likes it or not, the role the channel will play continues to polarise opinion.

Durgan Cooper, director of security and cyber risk at VAR Cetsat, said IT channel firms can help make cyber insurance a more effective option for end users by being actively involved in policy writing.

"[Channel partners] have to be involved because the client invariably doesn't know their security posture and an insurance broker is an insurance broker," he said. "He or she is not a technical analyst who can go out and identify where you're at risk.

"When you go to a proposal form for a cyber insurance policy, it asks you 'do you have a firewall?' It doesn't ask you 'what was the competency level of the installing engineer? What type of firewall was it? Was it a £ 1m Check Point (product) or was it a £ 59 PC World special?'

"It's a bit of a blank canvas in that it's not specific even to a vendor, let alone a technology."

This idea was however dismissed by Newman, who claimed that an understanding of the technical side of cyber insurance is not necessary to draw up an effective policy, adding that cybersecurity experts will never understand the insurance industry, in the same way that insurance experts cannot be expected to understand the technical side of cybersecurity.

"It's all rather ironic," he said. "If you think back to the physical security world, I don't have to have any clue how a fire alarm actually works in order to be able to provide building insurance. It doesn't matter one jot to me how that thing actually works."

"How does a sprinkler system work? I have absolutely no idea, but I don't need to understand that to be able to put together an insurance product and that is the problem."

"There's an assumption within the IT security market that you have to understand the bits and bytes, and how networks are structured to be able to provide an insurance policy - which could not be further from the truth."

Gottlieb agreed with Newman and said he does not expect channel partners to become more involved in insurance, purely because there is no opportunity to resell.

"Pretty much every client we have wants to know our opinion on it but what we usually see, especially from a channel selling perspective, is they often ask who we recommend, we'll give some advice and they'll say 'OK great, well our current insurer is AIG [for example] so we'll go and talk to them'."

"There is no resell opportunity for the channel really - no one is phoning up HP saying 'Can I buy an insurance policy from you?' They're going to continue with their existing direct insurance provider."

0 Comments

ChannelWeb

Carl Gottlieb

Recommend

Share

Sort by Best



Start the discussion...

Be the first to comment.

ALSO ON CHANNELWEB

Have we become over-reliant on AWS?

3 comments • 2 months ago

noooooooooon — S3 SLA is 99.9%, so whilst the downtime is a huge f'up, I suspect the business's hosting in one ...

Midwich snaps up Spanish distributor as spending spree continues

1 comment • 22 days ago

Muffin the Mule — Going places...

UKFast installs giant slide at office to encourage 'more fun and laughter'

4 comments • a month ago

Enjoy the Silence — The one-sided PR machine chugs on. How much did the slide cost one wonders...

Server revenue drops as enterprises stall - IDC and Gartner

1 comment • 2 months ago

Bruce — Companies are sweating their assets longer and doing more with less, as compute density increases. Also as ...

Subscribe Add Disqus to your site Add Disqus Add Privacy



© Incisive Business Media (IP) Limited, Published by Incisive Business Media Limited, Haymarket House, 28-29 Haymarket, London SW1Y 4RX, are companies registered in England and Wales with company registration numbers 9177174 & 9178013

