AUGUST 21, 2024

OBSERVATIONS OF A CISO – A SERIES OF OPINIONS

PRIVATE EQUITY COMPANIES & CYBER INVESTMENT RISK

thirty nine cyber 39

ASSESS. ADDRESS. **SUCCESS.**

HELP WHEN YOU NEED IT, NOT WHEN YOU DON'T.

OBSERVATIONS FROM A CISO

At ThirtyNine we recognise that the word of a salesperson isn't naturally accepted by many security professionals, there is a suspicion that there may be an endgame.
Unfair? Maybe, but it takes time to create trust, and we understand that.

So, we have decided to strap a keyboard to our CISO and let him run riot with his opinion.

These "blogs" are untamed and demonstrate how a cyber professional see's the world, oh and I might add stuff if I think its relevant as a director and founder of an SME to contextualise for non-technical readers.

We are always interested in your feedback, so if you have any please send them to our emails.

Gareth Stewart – Author: gareth.stewart@thirtyninecyber.com
Stuart Avery – Annoying Interloper: stuart.avery@thirtyninecyber.com

Private Equity Companies and Cyber Investment Risk

I've been chatting to a few Private Equity firms recently and there are a couple of interesting learnings that have come out of those conversations. These PE firms often have a number of portfolio companies under them, but they often don't have a mechanism or method to assess these for IT/Cyber risks.

One thing that surprises me is that cyber is often not considered as an investment risk (SA: is this because organisations believe that Cyber is an IT problem when actually it's a business problem?), or if it is there are limited ways they can properly conceptualise and understand this risk, much less turn that into a set of investment risks that can drive outcomes in a 90/100-day plan for example.

I've been on the "seller" end of a few bigger deals (100's of millions) and in those there was a strong element of due diligence for IT and Cyber security. Maybe these investments on the smaller end of the scale (sub $300M) do not feature such a strong due diligence process where it comes to Cyber (SA: If you think of your investments in aggregate, the total investment you have made may amount to this.), this I think is probably more down to a lack of understanding on how to assess these risks.

I'd think of this type of assessment as a "3rd Party Risk on Steroids" as if you're putting money, time, experience into a company in terms of an investment then you're going to want to understand ALL the risks and whether they are going to be at risk in 12 months' time of a big cyber incident that could potentially wipe away an investment.

A saying comes to mind "an ounce of prevention is better than a pound of cure". I think Private Equity firms should be mandating more of the cyber assessment pieces up front, where there is an assessment, and a programme plan developed to inject into the 90/100-day plan where there are relevant cyber risk mitigation strategies in place and the portfolio company's CEO is on the hook to deliver on this improvement plan (along with their other objectives). (SA: You may even ringfence some of the investment you make in the company to mitigate any cyber risks, that feels like good practice.)

Smaller companies are at the biggest risk of breach as they cannot afford to have a fulltime security leader at the helm, but they can have someone who can help and guide them along the way, this is something that the SME market in the UK needs.

(SA: If you consider that smaller innovative companies are producing game-changing IP for CNI and big company supply chains, critical to the wealth and growth of the economy, it's not surprising that they are considered a target for well-funded threat actors, the loss of this IP and the Brand Trust issue this causes for the target company can be catastrophic.)