KCS Group Europe

When, Not If

12/02/2018

There is a growing acceptance now that not only are cyber-attacks the greatest practical threat to today's business and industry, it is also a matter of *"when, not if"*. While top-level discussion is concerned about when Britain will suffer a *"Category One"* attack that cripples a crucial industry, businesses at all level of the supply chain must adopt this mentality of 'inevitability' as only this can spur them to taking the action that gives them the best chances of not avoiding an attack, but successfully protecting against it.

It is estimated that two 'significant' attacks hit the UK every day last year and that half of all businesses and institutions in the country were hit in total, many multiple times. Given the range, scale and abilities of the assorted cyber criminals arrayed against industry, stopping all of these is impossible – and equalled by naivety which assumes that there are so many tempting targets, your own business is unlikely to get hit. Only a total shift in mental attitude can provide the 'edge' to physical defences but this is so often lacking due to arrogance and ignorance over the true scale of the threat.

We erect fortifications – both physical and digital – because we fear attack and understand the need to put up some kind of defences. But never before has the question of inevitability been so strong. A band of marauders might consider the physical fortification of a medieval castle too much effort to storm, and move on to the next – just as some hackers will probe the defences of a cyber-system, decide it's not worth the effort, and look around for easier targets. Unfortunately, if one nowadays is dealing with hackers who are either being paid to get into a very specific system, or who have brought to bear their arsenal of social engineering, networking and ransomwaring to hit a company until it gives in, we no longer have this luxury. The barbarians are at the gates and they will not be leaving any time soon.

Does an attitude of inevitability mean blind panic and despair? Far from it. The attack might be inevitable but the outcome is far from predicted. With the right mindset, and defences, an attack can be repelled.

The most important strategy for “when, not if” is to ensure that you have all-round protection. There is little point protecting one side and leaving yourself exposed on the other. A firewall can only do so much, against a particular variation of the threat, and it is easy to fall into the trap of the “assured” protection this offers and assuming nothing else needs to be done. If accepting that an attack will happen, it therefore follows that it could happen by any means. What good is a drawbridge if the side gate is left open?

This must be matched by constant education about threats past, present and future: not just within the IT department but across the whole company. Again, the attitude of inevitability serves us well: if every individual is a target (which they are), how would they individually cope with having to take remedial action? It is not enough to know what can be done to recover from an attack, but to know what to do during an attack, to defend against it. If a business is resilient enough, it can withstand the threats. Repairing one gap in defences is far more practical, and possible, than rebuilding entirely.

This question of resilience is matched by one of long-term planning. An inevitable attack invites the requirement to know exactly what to do in a crisis, and how to get back on track afterwards. Indeed, any firm without a business crisis and recovery plan arguably cannot be taking ‘inevitability’ seriously enough. You hope it will never be used, but the likelihood is that it will be – is potential collapse worth the attitude of ‘let’s not bother’?

It ultimately is as much a mental attitude as it is a tangible effort. Only by accepting that the threat is real, that it is ever-present and that it will come for you can firms of any kind lay the firmest foundations for their defences. This was a lesson known 1000 years ago but which, in today’s new frame of conflict, seems to be lost.