+44 345 094 0945
www.waterstons.com

Article

Jan 2022

Ask these three questions to assess cyber risk in a business

My time as an IT Director and in mergers and acquisitions has led me to use a number of metrics as an assessment of the health of a business. These shortcuts are no substitute for a thorough understanding or for a due diligence exercise, but they are helpful in painting an initial picture. One might assess...

- The company's position compared to competitors
- Quality of the incumbent management team
- Free cash flows as well as EBITDA
- State of business control
- Percentage of business with individual customers
- Percentage of business which is repeatable and contracted

Some will be more important than others in each business or each M&A deal.

Cyber risk is now a matter for the audit committee and the board, not just for the head of IT. Therefore, an equivalent rule of thumb for cyber fitness is appropriate. If you are considering an acquisition, or starting as CTO with a company, you may want to ask these three questions:

1. Is all IT equipment on supported operating systems and regularly patched?
2. Is a copy of backups kept offline and are disaster recovery plans tested?
3. Is multi-factor authentication in place for all systems?

If an organisation can provide assurance of patching, offline backups and MFA in an early exploratory conversation, that says a lot about the integrity of its IT. This may seem a little 'techy', and it is no substitute for a full IT due diligence process, but it is a good indicator of sound business control.

A further benefit is that this trinity of controls is frequently used by underwriters when considering whether or not to place cyber insurance. A representative of one of the largest insurers said on an event I attended in December 2020 'if those three controls are not in place, we would struggle to provide cover.'