The Effective Board

INDEPENDENT
BOARD REVIEW

April 2014

# Cyber Stress

Driven in part by seeing other companies suffering pain and government pushing, directors are now very aware that “cyber risks“ need to be firmly on the board agenda.  But what should they be doing?  There can often be a reluctance to handle “IT things“ at board level.  Sometimes that‘s down to the directors lacking confidence in their knowledge of IT matters, and often through a feeling that if it‘s IT, it must be operational so it‘s best left to management.  But when it comes to “cyber risks“ (let‘s say that means threats to IT and data assets) it can‘t be avoided: the operational and reputational risks are just too big. So the Board does need to take a stance. Here we pick up on some of the basic steps you should follow.

| Good practices to consider... | Things to avoid... |
|---|---|
| Don't think that such a technical subject is beyond the Board's provenance or capability. The Board's job is to get assurance that the technical types are serving the business adequately, and for this you need objective critical thinking rather than deep expertise in technology. | Being bamboozled by the experts and supposing that if what you're hearing doesn't make sense then it must be because you don't understand it.  Or going to the other extreme and trying to dig into the details. |
| Get a proper understanding of the issues and risks in generic terms.  And don‘t just rely on your in-house view.  There‘s a lot of learning going on outside and you need to tap into it. Yes, get the internal briefing but ask how far this has drawn on external experience. And bring in some expertise from outside too to make sure the different angles are covered. | Being too internally-focused when getting to grips with the topic.  That way you only think in terms of your services, products and operations.  Possibly that will be enough but ideas or risks that have occurred to others may not spring to mind. |
| Ask how far your business is exposed.  And make sure the response is objective.  Of course look for a briefing from the Head of IT/CIO but make sure that there‘s an independent element.  If Internal Audit have got the expertise, they might fit the bill.  Or you may have to go outside. | Relying solely on the assessment of the Head of IT/CIO.  As “owner“ of the systems, they‘ll be confident that things are under control – but possibly over-confident?  “It‘s what we‘re already doing…“ might all too readily be the response. |

Assume that your defences will be breached. Until recently the typical response has been to build up the walls to stop anyone getting in. Now best practice is to assume they'll get in somehow. Or that the threat may come from within. So you need to tackle not just defence but, more importantly, resilience. So ask about the response to a problem, not just about attempts (probably ultimately futile) to avoid the problem in the first place.

Thinking it's all about not letting the hackers through and so asking only about penetration and defence, not about the response to breaches and managing the fall out. Or accepting assurances that you can't be penetrated. Current thinking suggests that complete security is unachievable.

Ask how the risk assessment has been done – and how far it's been appropriate for the business. You could well be operating numerous systems. And different areas of activity will have different risks (trading, transactional, retail, B2B…). Has IT's risk assessment taken these differences and the different structures and operations into account? And have you been helped to understand these different risks?

Simply accepting assurances that it has been done. And assuming that "one answer fits all". It may well be that IT have thought through all the dimensions – but you should check.

In looking to understand the risk analysis, resilience and response, think of "CIA": Confidentiality, Integrity, Availability of data and systems. It's a handy way of remembering that this issue has several different faces – but these three are fundamentally what it's about.

Failing to take a structured approach to asking the right questions – and being too general when talking about the risks. Unless you're an IT specialist (and there aren't that many of those at board level), framing the questions and thinking through the risks and response isn't easy. A framework helps.

Don't forget assurance. The system protections, policies and other risk management responses might be in place – but do they work? Will they hold up under stress? Do your audit plans cover the right ground – and do the auditors have the expertise to judge?

Assuming that the risk management responses are sufficient and will work when called on. They need testing in the same way as any other core controls and risk management systems – and checking by independent experts. If Internal Audit don't have the expertise, bring it in.

Think about reputation all the time. It's not only about operational down time – or possibly even fraud. It's about those nasty headlines or the embarrassment of apologising to customers and, quite possibly, the short and longer-term damage to the brand.

Focusing on the potential operational difficulties and losses. Of course avoiding or managing the operational fallout is key to avoiding any damage to your reputation. But the game is damage limitation so you need a contingency PR plan too.

Make sure you know the state of the "plan" – how far it covers the risks, the degree of implementation and whether it will stand up to the test. (Guidance standards from the BIS Cyber Essentials scheme are now available.) If necessary, commission senior-level expert advice to help you do this.

Failing to look at the plan. It's tempting to see this as the operational detail to be left in the hands of management. But in the same way the Board (or its Audit/Risk Committee) will look at the risk management plan in key areas, the cyber plan needs overseeing too.

Ask about what level of diligence can be reasonably expected from the Board – and possibly get some legal advice. There may be a level below which your insurance may be invalidated or other legal risks kick in. That could be around damages or possibly the Data Protection Act if the business is judged to have not taken reasonable steps to protect data and systems.

Relying on assurances that we're doing enough – and possibly that "it's not a big deal for us". If something does go badly wrong, one question to be asked is how far the directors took reasonable steps to ask the right questions and make sure management have done enough. And as directors you need to know the answer to "what's enough?"

Closer to home, think too about the confidentiality of board information. With widespread use of board portals, this is becoming less of an issue – but think about how much sensitive information flows outside of the corporate account and where it's going. What email addresses are you using and can you tighten your security by changing the set-up of your personal email account?

Just not thinking about it. We all probably sense that email isn't that secure. But if we take a hard and honest look at what gets sent to personal email accounts, we might well see gaps where we're exposed. And if someone was really determined to access corporate data, it would be a clear weak link.

If you have any questions on the issues covered here, please contact Chris Burt at chris.burt@independentaudit.com

This eBulletin is published monthly. To see back issues click here: "The Effective Board". To subscribe click here

We are leading specialist advisors on corporate governance. We assess the effectiveness of boards, committees, internal audit, external audit and risk management.

We perform full independent reviews. Or support your self-assessment or external facilitation using our web-based tool:

INDEPENDENT BOARD REVIEW A service from INDEPENDENT AUDIT LIMITED

www.independentaudit.com +44 (0)2072206580 Follow us on in

Independent Board Review is a trading name of Independent Audit Limited