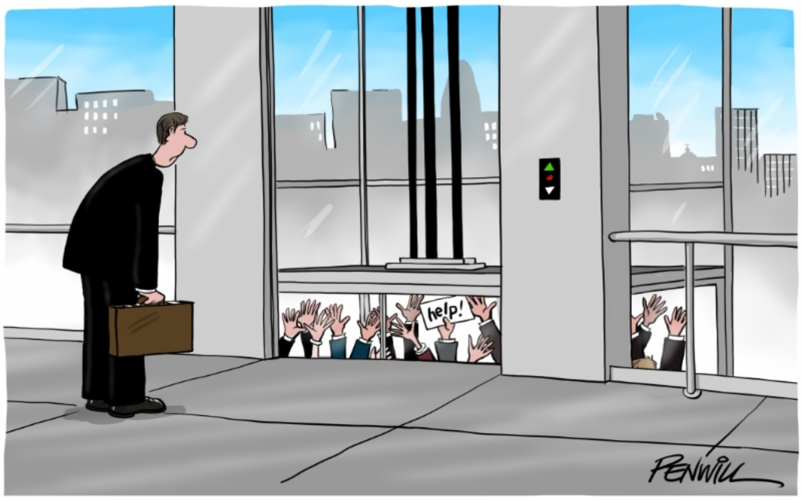
The Effective Board

INDEPENDENT AUDIT
BOARD REVIEW

March 2019

# Cyber risks - what a board should be asking



THE DIRECTORS WERE UNPREPARED FOR THE PRACTICAL EFFECTS OF THE CYBER-ATTACK SIMULATION

Something we keep coming across in our board reviews is cyber risk – and how a board can exercise oversight of this fast-moving and difficult to understand critical threat.  Most directors worry about the organisation's exposure, especially when they sense it's not a matter of "if" but "when". But few of them feel confident that their technical knowledge is sufficient to test what they are being told.  Are they merely forming a half-baked judgement on the adequacy of the mitigation approach or the organisation's ability to respond to a major breach?

It's one of those areas where directors can't be expected to become experts.  And finding someone who's already expert, but has the right profile to become a non-executive, will always be tricky – especially with such a limited pool to dip into.  In fact, increasing numbers of boards have stopped looking for cyber-NEDs and instead are appointing retained experts as their advisors.  But of course even those need to be used wisely by a board.  So, what's to be done?

At a minimum, the Board needs to have a clear framework of questions to ask – one based on a good understanding of the full breadth of the risk and required response.  Here we can touch only lightly on this complex topic.  But we have aimed to give a few pointers on good practice to help you cover the ground, and avoid the pitfalls.

## Good practices to consider...

Get a fully-scoped picture of both the types of risks and where they might hit.  Most boards are familiar with virus and hacking risks – but what about risks such as extortion, theft, information loss, espionage...?  And many have focused on the data loss but have a less than complete picture of the possible weaknesses in the operating structures, including the knock-on effects across operations, products and services.

## Things to avoid...

Just accepting the scope presented by IT.  They might not have the understanding of operational structures and processes that is needed to set it out in full – or of the potential hit on service delivery and customers.  NEDs need to hear from across the executive team, with each part of the organisation setting out their own scope of risk.  And once that's laid out, the NEDs need to stand back and use their experience and common sense to ask whether it really is a full picture of the significant risks.

Develop a framework for the Board to use in considering the possible costs and consequences. That means getting a picture of each area of impact – with the most significant, on a risk-based assessment, reaching the Board for discussion. And it needs to be wide-ranging, thinking through the consequences across the risk profile and risk register.

Thinking narrowly in terms of the cash-cost hit of an interruption to the operations. The consequences can impact the share price, reputation, fundraising capabilities and can create legal liabilities, health and safety incidents, failure to deliver contracts, regulatory fines… the list goes on. A board should be taking a look across its risk universe and asking how different types of hit might affect the risk assessment, and what that implies for the required mitigation approach and related investment.

Understand the exposures arising from third parties. The organisation itself might be on top of things, but where are the weak points in the defences that come from suppliers and outsourcers – and any others who have an interface with your systems? And get a good understanding of the positioning of the organisation around "open" or "closed" approaches to allowing data to be accessed by third parties.

Focusing on the internally-owned risks and risk management. The Board needs to be seeing a map of exposures and understanding how management are managing the risks. And assurance over those controls matters too – can the Board be sure that the mitigation is working well in practice, not just on paper?

Get a picture of how mitigation resources are being deployed versus the relative risks and potential consequences and costs. And then revisit the assessment as the risk environment changes.

Assuming that management are making the right calls on levels of investment and the targeting of resources. As always, NEDs should not be looking to second guess management. But they should be able to understand how management determine the appropriateness of investment levels versus risks, the checks and balances built into the decision-making, and how they keep on top of it all as the risks and the operations change.

Tie cyber risk considerations into strategic discussions and growth plans. New products, services, platforms, outsourcing, delivery mechanisms, partners, JVs, acquisitions, channels, geographies… they all have a cyber risk angle, especially if systems development or integration is involved.

Neglecting to think through the cyber risk implications of strategic decisions. It's natural for boards to look at the financial risk/reward balance – but are the cyber risks manageable and acceptable, especially when set against the projected returns?

Watch the geographical factor. New jurisdictions may change the game in terms of regulation, liability and control requirements – as well creating potential exposures in countries with

Thinking that, because all looks good at Head Office, we're on top of things. It's fully appreciated that different operating environments and cultures have to be factored into business-as-

| | |
|---|---|
| different standards or cultures around security or hacking. | usual controls and assurance approaches – but have they kept up with the cyber threat? |
| Understand the response plans for when a breach happens, and how they have been tested. That means understanding both the day-to-day responses as multiple attacks happen (nowadays part of business as usual) and how the organisation will respond to a major breach of the defences. To do this, it helps to have a clear framework for the Board to think within, covering the main categories (e.g. communication, customers, executive responsibilities, business continuity…) | Just accepting assurances that "we have a plan". The Board should be rigorously challenging its logic and looking for evidence of testing. Independent assurance will need to come into play – and if that means Internal Audit, do they really have the expertise? As well as covering the operational practicalities, is the external communication strategy clear? How will we look after our customers and stakeholders who are affected? A board needs to help management look above the internal challenges to make sure those outside are looked after. |
| Ask the "what if?". Boards who have tried wargaming a major breach typically find this helpful. Taking a close, up-to-date look at business continuity planning and testing is an obvious need too. | Being too accepting of assurances that "it'll be alright on the night". Boards can be just too accepting of the assurance they are given. It's not a question of distrusting what they are being told – it's just that these are not conventional risks and controls. It's new and it's constantly changing, so doubling up on the assurance over the defences may well be needed. |
| Get a clear picture of the critical systems. Boards can't be expected to look at the systems infrastructure in detail – but they should have a picture of critical systems and the cyber-related exposures. | Regarding the systems infrastructure as too operational and outside the scope of non-executive oversight. That might be the case for part of it – but where it is critical, it falls firmly to the Board to understand and to satisfy itself over the quality of risk management. |
| Take account of the human factor when looking at the control culture in relation to cyber risks. That means taking a look at how management are establishing the right values and behaviours: the messaging, training, support, monitoring, motivation and penalties. Also the Board should be asking executives about how they are reinforcing the messages along their management lines, from the CEO downwards. | Assuming it's enough that the control processes are sound and the policies in place. To an extent, regardless of firewalls and other defences, "it's all about behaviour". The human factor will always be a weak link. And do you really want to rely on the IT Department to look after this side of things? Behavioural initiatives have to be led by the CEO and executive team. |
| Understand the accountabilities. The Board should be clear about who is responsible for what. | Again, over-relying on the IT function. That might be where much of the practical defence activity is happening. But are the executives as a whole |

taking explicit responsibility for their areas of operations? The Board should have a good picture of executive commitment and ownership for what is an organisation-wide challenge.

**Working with CobWeb Cyber**

Independent Audit have teamed up with CobWeb Cyber (www.cobwebcyber.com) to help boards think through the questions they should be asking – and we acknowledge their thinking which contributed to this Bulletin. A questionnaire-based self-assessment will help your board think through how far it is covering the ground from an oversight point of view. To find out more, contact James Macaulay on +44 20 7220 6580 or at james.macaulay@independentaudit.com.

Independent Audit are leaders in board evaluation. We help clients understand and improve how well their governance is working.

If you have any questions on the issues covered here, please contact Richard Sheath at richard.sheath@independentaudit.com

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

To receive this bulletin regularly click here.

**www.independentaudit.com**

**+44 (0)20 7220 6580**

Registered in England number: 4373559
Registered office:
One Glass Wharf, Bristol BS2 0ZX