GOVERNANCE
March 2019 Issue 295

## Measuring governance

'Instead, the findings show that firm specific factors account for most of the differences. Firms with more cash, higher market-to-book ratio, and more intangible assets demonstrated the greatest cost impact from the conflict of interests.'

*Boris Nikolov, Erwan Morellec, and Norman Schürhoff*

## Cyber risk

'There must be a challenge to the current status quo. Boardrooms have become over-reliant on technical teams for advice and, as a result, restricted in how they can manage cyber risk from a strategic level. If controls are maintained only at operational level with no foundational strategy to maintain them then the overall cyber resilience is likely to be flawed.'

*Neil Hare-Brown*

# Content

# Feature

# Cyber risk

**Neil Hare-Brown** considers how boards should tackle cyber crime and suggests seven key strategies forming the foundations for effective cyber risk management.

The frequency and severity of cyber attacks are on the rise around the world. Such crimes include data breaches, fraud and extortion, raising the prospect of serious reputational damage. Yet many business leaders have questions about whether their organisations are adequately protected from a potential attack, and whether they are using best practice risk management tactics to drive down their exposure to cyber incidents.

Over the years, many board members have requested a non-technical list of things needed to manage cyber risk effectively. Cyber security standards and best-practice are often considered to be positioned for an audience engaged at tactical and operational levels and difficult for boards to digest.

Put simply, effective governance means managing cyber risk.

Growing numbers of executive and non-executive board members want a jargon-free list of key items they need to consider so that their businesses can manage cyber risk effectively. Yet, all too often cyber security standards and best-practice are considered too complex and technical for boards to effectively digest.

Those to whom they make such requests include senior and mid-tier management of information technology services as well as auditors, business consultants, industry associations and groups. They also look to relevant regulatory and government bodies such as the UK National Cyber Security Centre (NCSC).

In order to manage cyber risk effectively, boards need to understand, implement and monitor key strategies. They should *not* be concerned with tactical and operational level controls which, whilst also vitally important, use technical jargon which takes years of subject matter experience to understand and master.

Analogous to a military hierarchy, whilst a General may need an appreciation of the challenges in the positioning and use of artillery, they may not be best serving the effort if they spend most of their time on the front line.

*'Tactics without strategy is the noise before defeat.' Sun Tzu.*

**The problem with the cyber narrative**

Whilst the general approach from the cyber community is to both evangelise and attempt to empower board members with knowledge of the technical aspects of cyber security, this is rarely effective or practical. Often, the messages are considerably 'off-target' in that whilst they headline with subjects such as *No things the Board should do* and, *Key Cyber Security Issues for the Board*, the actual guidance remains far from strategic and aimed at the tactical and operational levels; often technical and packed with jargon which is likely to fail to engage board-level attention much beyond the headline.

Whilst extremely valuable, standards and certifications such as UK's Cyber Essentials, the Payment Card Industry Data Security Standard and the International Standard for Information Security Management, ISO 27001, are largely concerned with tactical and operational level controls within a business.

What board members really need is a way to assess the key strategies which form the foundations of good cyber risk management; not training on tactical or operational controls. Boards are well-used to being in control of several strategies as *business levers*, which they adjust, measure and feedback. They need to know how to operate these same levers to have the confidence that cyber security controls are mandated, operated and monitored in the most effective way possible.

There must be a challenge to the current status quo. Boardrooms have become over-reliant on technical teams for advice and, as a result, restricted in how they can manage cyber risk from a strategic level. If controls are maintained only at operational level with no foundational strategy to maintain them then the overall cyber resilience is likely to be flawed. A common example is key man-reliance, where the maintenance of security controls is reliant on just one or two key staff with no strategy to replace their skills should they leave. The risk of that key employee quitting only increases if they are not fully supported.

It is time for the cyber risk advisory narrative to change. Rather than educating boards about the technicalities of operational cyber risks, let's engage executives with useful, strategic thinking and, let's do so using business language.

**Explaining the Cyber|Seven Strategies**

For years, we have collected key observational data from hundreds of cyber incidents to which we have responded. The data is rich because it originates not from surveys but from first-hand management of cyber incidents where we have had the opportunity to engage directly with board members as well as technical specialists. We have analysed this data

# Feature

and identified *seven key strategies* which, if overlooked will significantly expose an organisation to high levels of cyber risk.

The *Cyber|Seven Strategies* are non-technical actions; explained using business language that any competent board will understand and be able to implement.

To our knowledge, this is the first time that straight-forward business strategies have been presented to help boards manage cyber risk effectively and to make their organisations more resilient.

Business leaders are increasingly realising that effective cyber risk management and resilience is not just about technology. Other important protections including high-level sponsorship, budgeting, staff resourcing, specialist skills, staff awareness, control over payments and cyber insurance.

Because the insurance portfolio of an organisation is usually the responsibility of a board member, it is vital that the *Cyber|Seven Strategies* are assessed and monitored by the same executives who decide on appropriate risk transfer.

To enable boards to 'self-assess' their organisations effective implementation of the *Cyber|Seven Strategies*, they must consider the points below and determine whether their businesses perform adequately in adopting these key strategies.

Once boards assess, adopt and monitor the key *Cyber|Seven Strategies* they will be supporting significant other good cyber risk management and security practices at both tactical and operational levels within their organisation.

**What are the Cyber|Seven Strategies?**

The key strategies forming the foundations for effective cyber risk management are:

1. *Responsibility*
Effective cyber risk management needs ownership: Boards must appoint a 'Cyber Champion' who is responsible for oversight of cyber risk management (budget, staffing, SLAs, security protection, cyber incidents, cyber insurance).

2. *Information asset awareness*
Boards must be aware of their intangible (data/info) assets and ideally sort them into broad categories and criticality.

3. *Adequate IT budget*
Notoriously under-funded by boards. Information is the lifeblood of pretty much all modern organisations and information technology needs adequate funding to ensure resilience.

4. *Payment control*
Because many payments systems are now online and almost all cyber crime is simply cyber-enabled fraud, payment controls such as segregation are more important than ever.

5. *IT staff count ratio*
The ratio of IT staff to end users: Too many organisations are massively understaffed leading to stressed IT teams who make silly mistakes and leave organisations vulnerable to cyber attack. IT staff and cyber security staffing is a key risk management strategy.

6. *IT skills & staff awareness*
Most organisations considerably under-invest in on-going training for IT staff; in standard IT, let alone cyber security. They need to support staff and make skills acquisition a pre-requisite for career growth and/or good job performance. Furthermore, all staff need to be given awareness training to enable them to spot cyber incidents and scams.

7. *Technology versions*
The older the technology the longer hackers have had to find vulnerabilities in it. Staying current means keeping the organisation ahead of the attackers. Boards do not need to know the details but do need a strategy which rejects suppliers who do not support the latest technologies.

As we have explained, whilst cyber security will always be a highly technical subject at tactical and operational levels of an organisation, it is vitally important that board members be engaged and informed on cyber risk management in a way which is more business-aligned and without technical jargon. Businesses need to consider whether they have sufficient and resilient foundational strategies which support the people, process and technology controls necessary to protect themselves from increasingly sophisticated cyber attacks.

Only by supporting the board to do what they do best will organisations begin to turn the tide on cyber criminals.

Take the board-level assessment here: https://www.cyberseven.global/

*Neil Hare-Brown is the CEO of STORM|Guidance, creators of Cyber|Decider, the cyber insurance comparator. STORM|Guidance are cyber risk management specialists with significant experience in fraud investigations and cyber incident response. We coordinate a leading cyber incident response team for a number of cyber insurers and manage hundreds of cyber incidents each year. STORM is an acronym for Strategic, Tactical & Operational Risk Management. It reflects our approach to understanding the best ways that cyber risks can be managed at each strata of an organisation's activities.*

GOVERNANCE
www.governance.co.uk

# Subscription form

**Please complete this form and send by mail to:**

**Subscriptions Department Governance Publishing and Information Services Ltd
The Old Stables, Market Street,
Highbridge, Somerset TA9 3BP, UK**

**Tel: +44 (0) 1278 793300
Email: info@governance.co.uk
Website: www.governance.co.uk**

**(Please tick one)**

☐ Yes! I would like to subscribe to Governance for one year

☐ Or, save with a 2 year subscription

**Governance international subscription costs:**

| | £UK | Euro | US$ |
|---|---|---|---|
| 1Yr | 325 | 450 | 490 |
| 2Yr | 585 | 790 | 855 |

Governance can accept cheques in other currencies but an administration fee of £15 will be charged.

| |
|---|
| ☐ I enclose a cheque/bankers draft for |
| Currency Value |
| ☐ Please invoice me |
| Specify currency: |
| Order reference: |
| Title: |
| First name: |
| Surname: |
| Position: |
| |
| Company/Organisation: |
| |
| |
| Address: |
| |
| |
| Postcode: |
| Email: |
| Tel: |
| Fax: |

# What our subscribers say

*'Governance* is a great publication that I look forward to reading.*'*

'I have found *Governance* to be a good resource for identifying and elaborating on emerging corporate governance trends.'

'*Governance* provides a very useful summary of key issues.'

'I enjoy *Governance* very much. The comprehensive range of topics covered keeps me up to date on corporate governance matters.'

'*Governance* is a useful means of keeping up to date on developments in a field which is assuming greater importance by the day.'

'*Governance* is the leading monthly publication covering major corporate governance issues. A most valuable source of information for investors, financial advisors, corporate board members and executives.'

# Index



**Designed and printed by**
**WithPrint**
Riverside Studio, Gills Lane, Rooksbridge, Somerset, BS26 2TY
**www.with-print.co.uk**

**ISSN 1358-5142**



**Governance Publishing and Information Services Ltd**
The Old Stables, Market Street, Highbridge, Somerset TA9 3BP, UK
**Tel: +44 (0) 1278 793300**
**Email: info@governance.co.uk Website: www.governance.co.uk**