www.pwc.co.uk

Governing cyber security risk: It's time to take it seriously

Seven principles for Boards and Investors

Dr. Richard Horne

Cyber Security Partner
PwC

January 2017

pwc

Board governance is often framed in terms of principles. I propose seven concise, but comprehensive, principles for the governance of cyber security to enable boards to 'step-up' their response to cyber security as an existential risk issue; explain their approach to stakeholders, and drive good practice.

The Corporate World needs to step up

Many boards recognise that cyber security is a risk that requires their specific attention.

However, most struggle to define a comprehensive board approach to cyber security – that genuinely manages risk rather than implementing 'standard' control frameworks in the hope they are sufficient. As a result, the question remains as to whether their response to cyber security threats is adequate.

From my board engagements in all economic sectors, it is apparent that there is a need for a pragmatic, recognised approach to governing cyber security risk that is grounded in practical experience.

There are many frameworks for the *management* of cyber security focusing on the definition and build of security controls. But there is little practical guidance as to what boards should consider in the *governance* of their organisations with regard to cyber security.

All organisations are different and each board needs to set its own direction and tone for cyber security. Given the nature of cyber security, this will impact all aspects of a business including strategy, business development, supply chain, staff and customer experience. In coming years, managing cyber security risk will potentially require radical change to businesses and their operations – to make themselves more *securable* as well as building security controls.

For this reason, a rigid standard would not be appropriate for governing cyber security, but a principles-based approach allows each board to establish and review its own direction within a recognised framework. Generic principles have been proposed by others, but a more meaningful, concise and comprehensive set is proposed here.

Investors are increasing their attention

Investors are becoming increasingly concerned about Cyber Security.

In PwC's 2017 *Global Investor Survey*, over 550 investment professionals gave their views on threats and opportunities facing companies. 73% of respondents identified cyber threats as an area of concern.

A landmark case in 2016 underlined how important cyber security is becoming for investors. Security research company MedSec partnered with investment firm Muddy Waters Research LLC to short sell stock in St Jude Medical Inc. They then disclosed what they claimed were security vulnerabilities in medical devices manufactured by St Jude. The claimed vulnerabilities were disputed by St Jude, and legal action was taken. Regardless of the outcome or ethics of the case, it is an illustration of the growing link between cyber security and company value.

An extreme example? Perhaps, but many other significant breaches such as that of Yahoo, that came to light in 2016, illustrate the potential damage to reputation and brand that can be caused, and even the possibility for corporate acquisitions to be impacted. Institutional investors are dedicating resource to research and probe cyber security risk management within companies they invest in.

However, feedback from investors is that discussions between them and boards on cyber security yield little clarity on a governance approach that extends beyond implementation of technical controls or often-vague discussion of 'risk appetite'.

A set of pragmatic principles for the governance of cyber security will provide structure for discussions between boards and investors. They will enable investors to ask more meaningful questions, and obtain greater insight.

Seven principles for governance of cyber security risk

In order to assist boards and investors, I propose seven principles for boards to adopt for the governance of cyber security.

The seven principles are that boards should ensure they, and their organisations:

1. Have a **real understanding of exposure;**
2. Have **appropriate capability and resource** dedicated to cyber security;
3. Adopt a **holistic framework and approach,** including meaningful measurement**;**
4. Submit to **independent review and test;**
5. Have sufficient **incident preparedness and a track record** of identifying, responding to, and learning from, incidents;
6. Have a **considered approach to legal and regulatory environments** for cyber security, and
7. Make an **active community contribution.**

These principles are briefly described below, and examples of factors to be considered for each are listed in the table that follows.

Consideration of these principles would enable boards to:

- Structure their governance of cyber security risk;
- Debate and make the tough decisions required (both by management and boards) to build an adequate response to cyber security threats;
- Challenge themselves and their executive management as to whether their response is adequate and evolving sufficiently rapidly as the risk develops;
- Structure a discussion with investors as to the appropriateness of their management of cyber security risk;
- Engage with investors to help them compare and contrast differing approaches to the management of cyber security risk, and
- Facilitate a discussion as to what would be appropriate for companies to report publically with regard to cyber security.

1 Real understanding of exposure

Many organisations fail to understand properly why they might be targeted; what might make them vulnerable, and how a successful attack might impact them.

The understanding needs to extend beyond the enterprise. It must reflect relationships that could make them a target and the complexity of digital connections that could cause them to be vulnerable: suppliers, service providers, partners, cloud services, critical data feeds, staff and customers to name a few. It must also reflect what data the organisation manages, why and where.

Building this understanding, and ensuring it stays current, is critical to ensuring that the response to the risk is adequate.

2 Appropriate capability and resource

Effective cyber security requires capable skilled resource that is empowered and resourced to shape an organisation to be secure. Boards need to be confident in the capability of their security function and its leadership, their ability to drive a broad response to cyber security across the whole enterprise, and rapid access to wider capability when required. Effective executive ownership is critical, with the CEO taking an active role.

For boards to be effective in this area, they themselves require sufficient capability to probe, challenge and support management. Board-level time needs to be devoted to drilling into detail, since that is where significant issues can lie. Capable non-executives are required, potentially supported by a board sub-committee with additional expertise.

3 Holistic framework and approach

A holistic approach to managing cyber security needs to not just build and operate effective cyber security controls. It must also reduce the complexity of the technology and data estate to which those controls are applied (inside and outside the organisation); address process and cultural/human vulnerabilities that attackers are increasingly targeting, and embed cyber security consideration in all business decision making.

Process vulnerabilities are often overlooked, but common targets. Examples include weak registration processes to online services or distributing sensitive data to an inappropriate third party for processing. A simple, but often exploited human vulnerability is poor password management, such as reuse of credentials across applications.

Recognised frameworks, such as those published by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) can help define required cyber security controls, but taking a broader approach is critical. Meaningful measurement is crucial, not just of controls but also extent of exposure.

4 Independent review and test

As with other significant issues, boards require independent validation and testing of their believed cyber security posture. This is achievable through independent expert review of cyber security frameworks and approaches, and even certifications of specific elements.

Strength of individual critical controls and systems needs to be tested and techniques such as 'red team testing' by skilled penetration testers can assess effectiveness of overall response to specific likely attack techniques (but only at a point in time). The speed with which issues identified through independent review and test are resolved should be measured.

5 Incident preparedness and track record

Cyber security incidents are inevitable. Governance of cyber security risk is important but effective governance when the risk materialises is critical.

Ensuring that focussed, practiced plans exist to respond to, and recover from, the most likely scenarios is essential. These need to consider not just technical resolution, but also business management, reputation management and management of legal and regulatory risk. Incidents need to be tracked, accurately reported, and lessons learnt.

In addition, organisations need to be able to respond appropriately to the reporting of vulnerabilities that could make products, services or internal processes vulnerable to attack.

The approach to incidents and vulnerabilities needs to be considered through suppliers and service providers, and not just within the 'perimeter' of the organisation itself. Exercising response at all levels is crucial, including the executive committee and board.

6 Considered approach to legal and regulatory environment

Cyber security cuts across an increasingly complex legal and regulatory environment globally. Industry regulation, data protection regimes, national security legislation, reporting requirements and product liability are a few examples of legal and regulatory environments that need to be understood, and a considered global response developed and maintained.

7 Active community contribution

No organisation can protect itself in isolation. Attackers commonly breach one organisation in order to target another, and replicate successful attack techniques rapidly. Thus collaboration is essential: between organisations within industries; through supply chains; between public and private sectors; between companies and law enforcement/intelligence agencies, and even with customers.

Examples of factors to be considered for each principle

Real understanding of exposure

- Clear view of data and processes – and products if relevant – that might be targeted
- Clear view of data, processes and products that might have disproportionate impact if breached
- Clear view of geographies that might heighten risk, and approach to 'segmenting' business and technology
- Broad and deep view of risks introduced through supply chain and approach to managing them (including integrity of data feeds that are relied upon)
- Understanding of customers that might heighten risk
- Understanding of how corporate culture might impact cyber security risk
- 'Threat Intelligence/situational awareness' – understanding of who might target the organisation, for what gain and likely attack types
- Embedding Cyber Security in other risk types, including quantified appetite for risk events caused by cyber breaches where appropriate
- Approach to wider risk mitigation (e.g. accurate understanding of what cyber breach coverage is provided by insurance policies)

Appropriate capability and resource

- Approach to ensuring appropriate board capability (e.g. expertise of NEDs, skilled board subcommittee, etc.)
- Sufficient board time devoted to drilling in to cyber security – both at main board and subcommittee level
- Clear executive committee accountability
- Credentials and experience of the leader responsible for cyber security and their reporting line
- Size and skill of security team
- Appropriate use of outsource providers to supplement skills gaps, provide 'burst capacity' (e.g. during incidents)
- Extent to which the organisation provides industry leadership for cyber security matters
- Turnover of key roles
- Approach to setting, reviewing and protecting budget for building and operating cyber security controls

Incident preparedness and track record

- Transparency over incidents and significant vulnerabilities – including in supply chain and service providers
- Approach to ensuring root causes of incidents are understood
- Speed of remediation of issues identified by incidents and vulnerability reporting
- Crisis plan ready and exercised, including: detailed 'playbooks' for most likely cyber security incidents; clear decision rights, and communication priorities
- Process for the reporting, qualification and remediation of potentially high-impact vulnerabilities (in products, services or business processes)
- Evaluation of 'near misses' – technical breaches with minimal impact that could have had significant impact
- Clear 'triggers' for escalation to executive and non-executive board members

Holistic framework and approach

- Cyber Security consideration embedded in Board and executive committee decision making processes
- Holistic approach to cyber security embodying people and processes – not just technical controls
- Structured reporting and measurement framework
- Clear decision framework for reviewing and accepting changes to cyber security through business developments (e.g. new products, geographies, M&A activities, completing integrations, outsourcing, high-risk customers)
- Recognised framework used for ensuring completeness of security controls (e.g. NIST or ISO27001)
- Approach to managing proliferation of data
- Approach to managing risk from supply chain and other external connections
- Complexity of technology and data estate (both internal and outsourced/cloud)

Considered approach to legal and regulatory environment

- Understanding of complexity of legal and regulatory environment in which organisation operates (e.g. differing national environments for: national security, law enforcement, privacy, reporting, product and service liability)
- Considered response to the legal and regulatory environments
- Coordinated reporting to (and influence on) regulators where appropriate
- Oversight, and accountability for, relationships with law enforcement and intelligence agencies

Independent review and test

- Independent review of security and approach
- Testing of key controls (not just in IT)
- Independent 'red team' testing of security effectiveness
- Strength of internal oversight through 'three lines of defence'
- Speed of action to remediate issues identified through independent review and test

Active community contribution

- Approach to information sharing and 'industry protection' with others in industry
- Approach to upskilling supply chain
- Relationships with national law enforcement and intelligence agencies
- Support to global and national initiatives
- Approach to upskilling customer base if relevant

About the Author and PwC

About the Author

Dr Richard Horne is a specialist partner in PwC UK for cyber security, advising boards of global and national organisations on the subject. A recognised authority and press commentator on cyber security, he is also a board advisor to a number of early-stage cyber security companies. Prior to joining PwC, he led cyber security for a global universal bank, and was seconded to the UK government to help shape the national plan for cyber security.

Richard can be contacted at richard.horne@pwc.com, and would be delighted to receive comment or suggestions to improve the seven principles.

About PwC

With offices in 157 countries and more than 223,000 people, PwC is among the leading professional services networks in the world. We help organisations and individuals create the value they're looking for.

Our purpose is 'Building trust in society and solving important problems', and in today's digital world that requires a focus on cyber security.

We help clients across society to understand their cyber security risk; build and assure their defences; identify and respond to attacks, and to navigate the complex legal and regulatory environment for cyber security. For more information please visit www.pwc.co.uk/cybersecurity

170110-144818-CU-OS