HM Government

Cyber Security: balancing risk and reward with confidence

Guidance for Non-Executive Directors

December 2014

Contents

"Cyber Security matters to me because it fundamentally impacts the day to day activities of almost every individual and organisation. With technology positively influencing the flexibility, agility and global reach of our day to day business, it is vital that we seek to protect ourselves, our customers and our supply chain from the loss of personal or sensitive information. We also need to guard against the theft of intellectual property, damage to our reputation or brand and of course financial and commercial losses."

Sir Michael Rake – Chairman of BT Group

Cyber Security: balancing risk and return with confidence

There is now a higher expectation that boards have a handle on the critical risks to their business – and cyber risks are no exception. Non-Executive Directors in particular, as the independent conscience of the board, are well placed to challenge the status quo and ask probing questions in this area.

Do I *really* understand the cyber risks my company faces?

This guidance seeks to help Non-Executive Directors engage with board colleagues on the oversight of cyber risks. It offers Non-Executive Directors key questions to help their company prosper in the information economy age.

What is cyber security?

Cyber security can be described as the digital or human measures you can take to reduce the risk and harm to your company's information and information based systems through theft, alteration or destruction.

Information is the lifeblood of an organisation, and yet with increasing automation and the degree of interconnection of information systems, a compromise of information in one area could impact the entire organisation and its customers. Information is everywhere: from customer facing systems (e.g. ATM, point of sale, mobile phones), to business systems (e.g. research, intellectual property, management information) and operational systems (e.g. safety, protection, process control).

Do cyber risks matter to my company?

Yes, because my company's current and future competitiveness is dependent on its intellectual property.

Yes, because my company is reliant, or increasingly reliant, on its online service to customers.

Yes, because we share important information or data with suppliers, contractors or service providers (including cloud and IT security outsourcing).

Yes, because our company is pursuing or engaged in a corporate transaction where we face significant competition or interest from other companies or state-owned enterprises.

Yes, because we facilitate and manage financial transactions on behalf of our customers.

Yes, because we collect and retain personal information about our customers and employees.

Yes, because my company's operational support or process control systems are directly or indirectly accessible from the internet.

Cyber risks arise from your company's exposure to the rapidly increasing interconnectivity of information. The risks are indeed real, and it is perfectly sensible to assume these risks are emanating from people who have, or seek to have, access to your information or information-based systems both internally and externally. Please see an example here of a recent high profile corporate attack. The Government's 2014 Information Security Breaches Survey: Executive Summary provides UK breach statistics.

In all likelihood cyber risks **do** matter to your company, but with challenge comes opportunity. Stakeholders and partners are increasingly seeking reliable assurances around protective competency from each other. Those seeking that assurance from your company either now or in the future include regulators, investors, employees, customers, partners and lenders.

Can your company offer credible assurance about its cyber risk management?

"It matters to me because at a time when data is power, and when systems run through the heart of most businesses, no serious company director can afford to ignore cyber security. At a minimum, every board needs to understand the key areas of vulnerability, the mechanisms to block external attacks and the means of detecting and addressing any breaches. Almost all businesses, and their customers, are at risk – both financially and reputationally – and that risk is increasing. There's no time to waste."

Rona Fairhead – Independent Non Executive Director, HSBC

Questions I should ask myself:

1. **Does the board regularly discuss the level of cyber risk it is prepared to take, and how much it is prepared to invest in managing that risk?**

2. **Do I *really* know who is responsible for cyber risks in my company?**

   Have I met them and am I confident there is sufficient segregation between them and those making decisions about the technological direction of the company?

3. **Do I fully understand the board's cyber updates, briefings or papers, and how that information was generated?**

   Are the cyber updates and technical briefings clear enough to enable a strategic discussion which encompasses the wider corporate environment? Is the board investing too much trust in its technical staff when signing off options which may carry personal liability for each director? Do briefings cover the basic areas outlined in the Government's 10 Steps to Cyber Security guidance?

4. **Is the board being offered choices or options in relation to cyber risk management?**

   Regular IT driven updates will not aid effective board level oversight of the risk.

5. **Outside of board meetings, do I speak regularly to the Chief Information Officer, Head of Internal Audit or Chief Information Security Officer to improve my understanding of the company's threat profile, controls and processes?**

6. **Have I considered being a 'board room buddy' or sponsor for the Chief Information Officer, Chief Information Security Officer or Head of IT?**

   Can I help them communicate effectively with the board and vice versa around technology and business objectives?

7. **Do cyber risks form part of the assessment of risk for all new projects and transactions?**

   For example, cyber risks may be higher during the company's involvement in a high value transaction.

8. **Have I encouraged board colleagues to provide assurance to investors and customers?**

   Could a paragraph in our annual report boost investor confidence, whilst enabling us to enhance reputation and seize commercial advantage? I could suggest publicly presenting our Cyber Essentials certification.

9. **Am I confident the business is prepared for a major breach?**

   Is there an organisation-wide crisis management plan in place? Should I encourage the management team to present a tabletop cyber scenario to the board? Consider starting with the Government's 10 Steps to Cyber Security guidance (Incident Management advice sheet). Also see the Government's Computer Emergency Response Team, (CERT UK).

10. **Which board members are fluent in the risks and opportunities of the digital age? Are they actively educating and supporting their colleagues so the board as a whole can manage cyber risk?**

    Should we address the need for stronger technology and digital understanding (including cyber risks) through board education, NED recruitment, or better use of external risk management experts – or all three?

"It matters to me because the risks to company performance that I worry about are the ones that I don't know about. The lists in this cyber guidance better equip me to ask the right questions, to the right people, to uncover what I don't know and therefore work to ensure that the company is best-prepared."

Dale Murray – Technology entrepreneur and angel investor

"It matters to me because as chairman of a successful international business we cannot afford to compromise our critical information and data assets. As a board we have the responsibility to protect sensitive information we maintain on our system concerning our employees, our intellectual property and information on our clients"

Allan Cook, Chairman of Atkins, a multinational engineering company

Questions I should ask my board colleagues

1. **Have we identified and understood the value of our company's critical information and data assets? What is that small percentage of information within our business that makes it competitive?**

2. **Do we receive a regular update showing the threat to our business and critical data assets?**

   This could include threats and actual attacks in relation to physical, commercial, personnel and IT. Silos and poor management information will hinder your ability to draw a clear threat picture. I could ask whether the company is a member of the Cyber Security Information Sharing Partnership (CISP) which will help to improve situational awareness.

3. **What assurances do we have that adequate technical controls and processes (e.g. the 'basics') are in place to protect these assets?**

   If our company has the basic controls in place (e.g. the Cyber Essentials Scheme) this can prevent many types of common infection and compromise. A sophisticated and well resourced adversary will not waste valuable capability when a basic vulnerability will allow easy access.

4. **Do we have assurances that our staff, suppliers, cloud providers, contractors, overseas subsidiaries and partners can be trusted to safely access our critical information and data assets?**

   What credible assurances do we ask for? We could request Cyber Essentials certification. What assumptions have we made about our resilience to cyber risk, and do our business processes reflect this?

5. **Have we agreed a risk appetite statement for cyber risks and are we confident it is reflected in day-to-day decision making?**

   Strong financial performance can often mask the risks that are being taken. Setting a risk appetite can help balance the relationship between the speed of innovation and understanding of the risks.

6. **Have we considered in detail the potential resulting consequences to our business, both now and in the future, from the loss or disruption to our critical information and data assets?**

   We could explore commissioning some work to understand the financial impact of various forms of attack on the balance sheet and earnings of the company.

7. **Can we invite representatives from other areas of the business to participate in board level cyber risk management discussions (e.g. HR, legal)?**

   Cyber reaches across the whole business – personnel, physical security, commercial relationships, etc. We should not restrict the discussion base to the Chief Information Officer, Chief Information Security Officer or Head of IT and seek to include other parts of the business to listen and participate.

"It matters to me because we need to balance digital innovation with cyber risk. My boards are excited about the potential of the internet age; but with every exciting new internet- or data-enabled innovation comes new threats. We have had to find the skills, language and governance process to bring cyber into the boardroom where it belongs, as a new strategic and operational business risk."

Stephen Page - Non Executive Director focusing on boardroom leadership for the digital age

"It matters to me because much of the value in many of today's growth companies resides in digital assets and proprietary information stored in digital form. Dedicating time and diligence to ensuring adequate protection of virtual assets, preserving the continuity of online services, and avoiding information leakage, are all key parts of a board's responsibility to ensure risk mitigation."

Alan Aubrey – CEO of IP Group plc, a leading intellectual property commercialisation company

Questions I should ask at Audit or Risk Committee

1. **Are we measuring the degree to which we are meeting the board's cyber risk appetite?**

   Are there suitable Key Risk Indicators which show our risk and how it is being mitigated through technology, partnerships, corporate culture and people? How confident are we that those indicators are current and accurate?

2. **Do we periodically review our key information and data assets and are we clear about the threat to those assets?**

   Have we agreed an appropriate level of protection for our most business critical assets? Have we decided what NOT to protect?

3. **Is our operational risk and internal audit plan providing cover across different areas of cyber security (e.g. cyber incident response review), or is it just focused on IT operations?**

   Do we have the right skills and experience in-house to cover all areas?

4. **Have we assessed the capabilities and maturity of our peers?**

   We could use the findings from the Government's FTSE 350 Cyber Governance Health Check.

5. **Do we have a complete map of our network and connections to the internet, the operating systems and applications in use, and the number of users with administration rights?**

   To help limit insider threat to our information, we may want to audit the end-to-end processes which govern who uses our systems and what they are permitted to do – including the responsibilities of HR, line management, IT, suppliers and our workforce.

6. **Are we confident our network is sufficiently maintained and updated, and has it been tested?**

   Is our level of maintenance (e.g. patching) sufficient and acceptable? Are we using a clear policy for mobile devices and how they connect to our systems? Do we have a detailed understanding of which suppliers/partners connect to us and how?

7. **Which recommendations in our penetration testing reports have not been acted on, why not and for how long have they been outstanding?**

   Penetration testing is now very common and although it illuminates a problem, it is not a solution in itself. What broader conclusions about culture, governance, technology or business processes can we draw by looking at the root causes of penetration test issues?

8. **Do we have assurance that our software is up-to-date?**

   If not, we could be extremely vulnerable to cyber risks (e.g. Windows XP support has now ended).

Where to go for more help and advice:

Ten Steps to Cyber Security

The Government's primary cyber security guidance, which is designed to offer board rooms practical steps to improve the protection of their networks and the information carried upon them.

www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

CYBER ESSENTIALS

The Cyber Essentials Scheme

Cyber Essentials is a Government-backed and industry supported technical scheme to guide businesses in protecting themselves against cyber threats. The Cyber Essentials scheme provides businesses, large and small, with clarity on good basic cyber security practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. The Cyber Essentials badge allows your company to demonstrate that it adheres to a Government-endorsed standard. These technical essentials form part of the broader agenda described in the Ten Steps to Cyber Security guidance.

www.cyberstreetwise.com/cyberessentials/

Cyber Incident Response

Through a twin track approach encompassing a broadly based CREST (Council of Registered Ethical Security Testers) scheme endorsed by GCHQ and CPNI, and a small, focused GCHQ and CPNI scheme designed to respond to sophisticated, targeted attacks against networks of national significance.

www.cesg.gov.uk/servicecatalogue/service_assurance/CIR/Pages/Cyber-Incident-Response.aspx

CERT UK

CERT UK is the UK National Computer Emergency Response Team. CERT UK works closely with industry, government and academia to enhance UK cyber resilience.

www.cert.gov.uk

Cyber-Security Information Sharing Partnership (CISP)

The CISP facilitates the sharing of information and intelligence on cyber security threats in order to make UK businesses more secure in cyberspace. The CISP includes a secure

online collaboration environment where government and industry (large and SME) partners can exchange information on threats and vulnerabilities in real time.

www.cert.gov.uk/cisp/

The National Cyber Crime Unit (NCCU)

The NCCU, as part of the National Crime Agency (NCA), is the UK lead for the investigation of the most serious and organised cyber crime. The NCCU will support domestic and international law enforcement, and the wider NCA, to take responsibility for tackling cyber and cyber-enabled crime affecting the UK.

The NCCU will be accessible to partners; responding dynamically to threats, providing expert advice, guidance and feedback. The NCA is not a crime reporting agency, so any reports of crime should be reported to Action Fraud (see below).

www.nationalcrimeagency.gov.uk

Action Fraud

Action Fraud is the UK's single point for reporting all fraud and online financial crime. Crime can be reported online 24 hours a day, seven days a week, and the Action Fraud call centre can also be contacted to report crimes during working hours and at the weekend. When a serious threat or new type of fraud is identified, Action Fraud will place an alert on its website which contains advice for individuals and businesses to protect themselves from becoming victims of fraud.

www.actionfraud.police.uk

Centre for the Protection of National Infrastructure (CPNI)

CPNI protects national security by providing protective security advice, covering physical, personnel and cyber security, to the UK's Critical National Infrastructure (CNI). CPNI works to raise awareness at board level as well as at a technical level across the CNI. Cyber security advice and guidance is available on the CPNI website.

www.cpni.gov.uk

© Crown copyright 2014

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. Visit www.nationalarchives.gov.uk/doc/open-government-licence, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

This publication is also available on our website at www.bis.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000
biscybersecurity@bis.gsi.gov.uk

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.
BIS/14/1277