icsa
Trust through governance

Guidance note

Cyber risk

Contents:

Institute of Chartered Secretaries
and Administrators

June 2013

1 Introduction

The internet provides a largely anonymous and cost-effective method for those involved in organised crime, economic espionage, and other adversaries, to damage or embarrass companies. Those engaged in cyber attacks aim to secure economic advantage by stealing financial assets, intellectual property or critical information. This can be from a single serious event or a sustained attack over a period of time, sometimes years. The impact on a company as a result of being targeted in a cyber attack, including the impact on its reputation, can be catastrophic.

Managing cyber risk is a business-critical activity, and cannot be regarded as simply an IT issue. Cyber risk is different from other types of risk because of the rapid evolution of technology and the resulting fundamental changes in the way business is conducted. Boards will need to think differently and consider taking wider advice, to ensure they fully understand the issues faced by their company in order to manage the risks appropriately.

If you have any feedback on the content of these resources, or additional questions that you'd like to discuss, please contact the ICSA information centre: **020 7612 7035** | **informationcentre@icsa.org.uk**

The information given in this guidance note is provided in good faith with the intention of furthering the understanding of the subject matter. While we believe the information to be accurate at the time of publication, ICSA and its staff cannot, however, accept any liability for any loss or damage occasioned by any person or organisation acting or refraining from action as a result of any views expressed therein. If the reader has any specific doubts or concerns about the subject matter they are advised to seek legal advice based on the circumstances of their own situation.

2 Issues for boards

Security breaches within UK companies, large and small, continue on an upward curve. Of those organisations that responded to a 2013 survey, 93% of large organisations and 87% of small businesses experienced a security breach in the past year, with the main reason for the increase being cyber attacks. The cost of cyber security breaches against British business has tripled in the past year and amounts to billions of pounds annually.[1]

Key cyber adversaries include:

- organised crime by cyber criminals engaged in fraud or obtaining money or valuable information;
- employees who can cause damage by accident, or by deliberate and malicious misuse;
- competitors or foreign intelligence services that are interested in gaining economic advantage for their own companies or countries;
- computer hackers who enjoy the challenge of this activity; and
- hacker activists ('hacktivists') who wish to attack companies for political or ideological motives.

Cyber attacks are often public – but they are frequently not made public in circumstances such as where an organisation is blackmailed or defrauded. Attacks can be carried out entirely remotely, and companies may not be aware that they have been attacked for some time after the event. Some may never be aware they have been attacked. The threat of attacks from other nation states is growing rapidly as the capability of other countries to carry out cyber attacks increases.

Companies need be on the 'front foot' in terms of cyber preparedness, with the board having a firm grasp of the risks, to ensure a proportionate, business-wide, risk management-based response. The cyber threats facing businesses and their supply chains cannot be prevented through investment in technology alone. It requires comprehensive risk assessment processes to identify and prioritise the protection of critical information assets. Boards, with the assistance of the audit committee, should provide ultimate oversight of strategic and operational cyber risks, as they do other key risks.

[1] 2013 Information Security Breaches Survey: www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report.

Boards might find it helpful to focus on the following points:

- Understand your company's cyber risk. It is very specific to an individual organisation's situation, even within a single market sector.
- Make an active decision as to the balance between the risk the organisation is prepared to take, and the costs to be incurred in targeted spending, to protect the organisation from cyber attack.
- Plan for resilience. As threats become more sophisticated, focus on resilience to attacks that get through, rather than preventing all cyber attacks.
- Be clear who is responsible for owning the risk, allowing for the dynamic and sometimes targeted nature of a cyber threat. Boards may consider giving one director specific responsibility for oversight of cyber risk.

3 Why cyber risk is different from other risks

The risks associated with cyber activities are relatively new, and boards are unlikely to have a comprehensive understanding of the issues or have past experience of dealing with such risks. As a result of the growth in internet trading in recent years, companies may not be aware of their level of vulnerability. There is little sharing of information on cyber attacks between organisations and, unlike other risks, there are active enemies directing their activities towards damaging companies. As a consequence, boards may need to spend more time ensuring they are fully informed, and have a complete understanding of the cyber risks faced by the company. Boards should be aware that, if their strategy is dependent on technology, which is increasingly the case, the stability of the company's operations is at risk from cyber attack.

Without a full understanding of the risks, companies may focus their attention and spending on areas that do not reflect the greatest risks. A lack of understanding of the issues often results in an inappropriate response, such as simply increasing levels of IT security. Robust IT security needs to be combined with a properly- structured control environment.

4 Assessment and management of cyber risk

The business case for managing cyber risk is clear. A comprehensive, business-wide risk assessment is critical, covering both current and emerging risks. The risk profile will be different for all organisations, and risks should be assessed as both strategic and operational. The level of risk tolerance a company is prepared to accept should be set by the board and this, together with the management of cyber risks, needs to be based on full information on the vulnerability of the company, and the consequences of cyber attack. Resources can then be deployed in the most crucial areas and in the most cost-effective way. Control procedures should be monitored and reviewed regularly by the board to assess their effectiveness, and should include the appointment of key risk individuals who are ready to respond quickly to minimise the consequences of any cyber attack. Regular assessment of identified cyber attacks will show where internal controls and procedures have broken down and need to be improved.

4.1 Understanding cyber risk

The main challenge is that there are many types of cyber risk, and each company will have a different combination of risks associated with their specific cyber threat. Set out below are five categories of cyber business risks, which can occur separately or overlap.

1 Censure and embarrassment

This impacts the company's brand through negative publicity, and can cause a major disruption to strategy. It is most relevant in highly visible industries such as retail, finance, media, or law and can be as a result of hacktivism. Regulated industries may also suffer additional negative publicity as a consequence of subsequent regulatory censure.

2 Client loss

A reduction in revenue can result from customers abandoning and/or suing the company following a loss of service or confidential information. Sectors where companies store information on behalf of customers, such as IT or professional services, or any retail business, are most at risk from client loss.

3 Direct fraud

Theft of money or digital content by electronic means is most relevant to financial services operations and those whose products can be copied online, such as media and software companies. Examples are the stealing of card numbers to withdraw cash, or copying music.

4 Sabotage or disruption of business operations

This most commonly manifests itself as the disruption of services to customers, and sometimes involves blackmail of online businesses. There is also the possibility of cyber terrorism against industrial organisations such as energy and utilities, where control systems are connected to the internet.

5 Cyber espionage

The silent copying of information for commercial purposes is most relevant to industries with high research and development costs, such as high-tech manufacturing, aerospace and software. It can also affect companies competing for high-value contracts in areas like construction or mining. Any company involved in merger and acquisition activity is vulnerable.[2] This is typically not reported directly but is common and large-scale.[3]

4.2 Assessment of risk

- Initial assessment of the organisation's risk profile, and whether it is particularly vulnerable to attack, is crucial. Companies may not have sufficient experience internally to gain this full understanding and find appropriate solutions, so it is often beneficial to include external advice as part of the assessment. Any reports received from external advisors should be clearly written and easily understood by all.

- Risk assessment should be carried out across the whole organisation, to assess the overall risk and identify specific areas at greatest risk. Internal functions such as HR, finance, legal and marketing may not appreciate the extent to which critical information is at risk, nor realise the potential impact of a cyber attack on their organisation.

[2] http://bloom.bg/1axVdsb
[3] http://bit.ly/10zlPYI (Paragraphs 25 and 26)

- Risk assessments need to concentrate on the threat to the protection of information, including customer data, and focus on the potential consequences which include losses from a substantial interruption to online transactions. The potential for the destruction of corporate value should not be underestimated.

- Assessment should include the risks of using third party providers and the company's supply chain. Outsourcing can sometimes be a more secure option, but it requires thorough due diligence in advance. Service providers may hold a great deal of valuable company information, so adversaries can obtain information without the need to attack a company directly. It should be remembered that, whilst companies can outsource activities, the risks, and the consequences, remain with the company.

- Risk reports and risk registers provided to the board and audit committee should include full and comprehensive information. Reports should reflect a fuller understanding of the impact of a cyber attack, including the wider impact on future strategy. As with all information received by the board and board committees, the company secretary has a role in ensuring the quality and quantity of information provided on cyber risk. It is essential that the risk function ensures the risks identified are communicated and understood by all areas of the organisation that could be affected by the risks, and that the board's priorities for mitigating cyber risks are communicated to all business areas.

5 Action for the board and the audit committee

Boards need to ensure all aspects of effective governance are in place, which includes receiving full information and having clear oversight of the cyber risks faced by the company. The board should speak directly to the Chief Risk Officer, or equivalent, who should have a good understanding of the cyber attacks being experienced across all parts of the business. Day-to-day control of cyber risks should not be left to the IT department. The Board should challenge those responsible for cyber risk to satisfy itself that a thorough assessment has been carried out and that risk management procedures are robust.

Cyber risk

When reviewing the risk assessment, the board and audit committee should focus on the consequences of a cyber attack. The key risks to the company need to be assessed and priority given to risks of strategic importance and those with implications for the company's reputation, together with risks involving contractual issues, and the possibility of exposure to regulatory breaches. However, information received needs to be considered in the context of future strategy, to obtain a clear picture of the risks to the company from cyber attack.

Boards may wish to challenge management to be able to answer the following key questions as they seek to improve their cyber security:

Protection of key information assets is critical

i) How confident are we that our company's most important information is being properly managed, and is safe from cyber threats?

ii) Are we clear that the board's directors could be key targets?

iii) Do we have a full and accurate picture of:

- the impact on our company's reputation, share price or future survival, if sensitive internal or customer information held by the company were to be lost or stolen;
- the impact on the business if our online services were disrupted for a short or sustained period?

Exploring who might compromise our information and why it is critical

i) Do we receive regular intelligence from the Chief Risk Officer (or equivalent) on who may be targeting our company, their methods and their motivations?

ii) Do we encourage our technical staff to enter into information-sharing exchanges with other companies in our sector and/or across the economy, in order to benchmark, learn from others and help identify emerging threats?

Cyber risk

Pro-active management of the cyber risk is critical

i) Cyber risk potentially impacts share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology, and finance. Are we confident that:

- we have identified our key information, and thoroughly assessed its vulnerability to attack;
- responsibility for cyber risk has been allocated appropriately on the risk register;
- we have a written information security policy in place, which is championed by us and supported through regular staff training;
- the entire workforce understands and follows the policy?

Do we understand the consequences of failure:

i) to the company's financial stability;
ii) to the company's brand and reputation;
iii) to the company's future strategy; and iv) to the potential for corporate failure?

Further guidance

Further guidance for companies on how to manage cyber risk can be found in the Government's *Cyber Security Guidance for Business*:
www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

The *Cyber Security Guidance* pulls together Government expertise in an accessible toolkit to support businesses in dealing with the growing cyber security threat. The Guidance is designed to offer practical steps which companies can take to improve the protection of their business assets from technical, commercial, and financial threats.

Working group

This Guidance Note has been prepared with the assistance of a working group comprising industry experts on cyber risk from the Department for Business, Innovation and Skills (BIS), Airmic Ltd, BAE Systems Detica, In Command Ltd and ICSA Members who are company secretaries of FTSE 100 and FTSE 250 companies.

icsa

Trust through governance

ICSA is the chartered membership and qualifying body for professionals working in governance, risk and compliance, including company secretaries.

We seek to develop the skills, effectiveness and profile of people working in governance roles at all levels and in all sectors through:

- A portfolio of respected qualifications.
- Authoritative publications and technical guidance.
- Breakfast briefings, training courses and national conferences.
- CPD and networking events.
- Research and advice.
- Board evaluation services
- Market-leading entity management and board portal software.

Guidance notes are prepared by the ICSA policy team to support the work of company secretaries and other governance professionals working in the business and not-for-profit sectors, and in NHS trusts.

Guidance notes offer authoritative advice, interpretation and sample materials for the many issues involved in the management and support of boards. As such, they are invaluable for those helping their organisations to build trust through good governance.

There are over 100 guidance notes available to ICSA members at **www.icsa.org.uk/guidance**

The Institute of Chartered Secretaries
and Administrators
Saffron House, 6–10 Kirby Street
London EC1N 8TS

June 2013

Institute of Chartered Secretaries
and Administrators