Deloitte.

November 2015

# Governance *in brief*
# Is your organisation prepared for a cyber-attack?

**Headlines**

- Cyber-attacks are already inflicting substantial damage on organisations today; including disruption to operations and reputational damage, resulting in erosion of customer trust and falling share prices. The volume and sophistication of these attacks continues to increase.
- Many organisations have not taken the steps to protect themselves adequately against these attacks and are insufficiently prepared to respond effectively when they do suffer an attack.
- Boards need to ensure that cyber risks are being considered appropriately, and should seek to understand how secure, vigilant and resilient their organisations are:
  - **Secure:** Are the right controls in place to prevent both known and emerging cyber-threats?
  - **Vigilant:** Do we understand how cyber-threats are changing? Are we confident we would actually know if we had suffered a cyber-attack?
  - **Resilient:** How well prepared are we to deal with a successful cyber-attack? Have we planned and practiced how we would recover?

## A very high profile threat

Recent media coverage of high profile cyber-attacks continue to highlight the damage that hackers, cyber criminals and disgruntled employees can cause to organisations. Cyber-attacks cause not only the obvious business disruption, financial fraud and customer data loss, but can also lead to longer term business problems such as those arising from reputational damage and industrial espionage.

Most reports on cyber security revolve around a common theme, which is; despite unprecedented levels of security investment, the number of cyber incidents and their associated costs continues to rise. Reports typically point to the growing sophistication of hackers and other adversaries as a particularly intractable problem, and some consider whether being secure is even possible in today's rapidly evolving cyber landscape.

## Understanding the threat

Part of the underlying reason for the trend of increasing cyber-security incidents and associated costs is that we have woven a fabric of connectivity in our economy and society via the Internet; a platform that was designed primarily to share information, not to protect it.

Your organisation has doubtless benefitted from this connectivity, driving innovation, efficiencies and performance that were unthinkable a generation ago. For example, you may have transformed relationships with customers and suppliers, removed geographic constraints, automated diverse operational systems or enabled your people to work from anywhere at any time.

The benefits this connectivity brings you also add complexity, volatility, and dependence on infrastructure not fully within your organisation's direct control. This introduces new gaps and opportunities that attackers will try to exploit. For every step you take to exploit the Internet, your adversaries are close behind. In short, as your sophistication in exploiting the Internet grows, the sophistication of cyber-attacks you face does too.

## Tackling the threat

Protecting everything, while perhaps not impossible, would be economically impractical and would likely impede some of your most important strategic initiatives. In other words, your cyber controls are necessary, but in isolation not sufficient. Your approach needs to acknowledge that some cyber incidents will occur and therefore that the traditional discipline of security, isolated from a more comprehensive risk-based approach, is not enough.

Through the lens of what is most important to you, you need to invest in cost-justified security controls to protect your most important assets. However, you also need to focus at least equal, and in some cases greater effort, on gaining better and faster insight into threats, and responding more effectively to reduce the impact of a cyber-attack when it does occur. Responding effectively includes developing an ability to rapidly determine the scale of any damage caused by an attack, dealing confidently and accurately with customers, shareholders, regulators and the media, whilst restoring business operations safely and effectively.

### Key areas of consideration

*Robust assessment of the risk*

- Who is likely to want to launch a cyber-attack on us, and why? How is this likely to evolve in the future?
- What are the most critical assets we need to protect from a cyber attack? How did we assess this?
- Do we understand the impacts of a successful attack on these assets?
- Have we defined a cyber risk appetite? How?

*Monitoring of internal controls effectiveness*

- Who is responsible for managing our risks associated with cyber?
- Are our controls to prevent cyber-attacks effective and in line with our risk appetite?
- Do we have the right intelligence mechanisms in place to understand rapidly how the cyber-risk is changing? Can we rapidly alter our controls as a result of this intelligence when needed?
- Are we confident we would detect a successful attack? Have we developed and rehearsed how we would respond to a successful attack?

*Management and mitigation activity*

- How do we ensure that our people, including the Board, are trained appropriately regarding cyber risks and their responsibilities?
- How do we compare to our competitors, other industries and relevant cyber security standards?
- What is risk, internal audit and external audit's role in assurance around cyber?

### Deloitte view

- Audit Committees need to act as catalysts to ensure that their companies are well informed about the cyber-threats they face, the most important information assets and systems to monitor and protect, and how they would respond to a successful attack.
- Boards have a duty to report to shareholders on the principal risks, including cyber-threats, and how they are being managed or mitigated, to monitor material controls and to perform an annual review of effectiveness. Careful consideration should be given to the description of these activities to ensure that, in this rapidly evolving area, companies avoid giving the impression of total resilience or fully effective controls.

### To discuss this topic further

Deloitte's Cyber Risk Practice assists organisations throughout the public and private sectors with their cyber challenges, including cyber assessment and strategy, implementing cyber-defences, providing threat intelligence and managed cyber services and helping organisations deal with the aftermath of a breach. For further information about the practice, please contact Nick Seaver (**nseaver@deloitte.co.uk**) or Phill Everson (**peverson@deloitte.co.uk**).

### The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training.

The briefings are pitched at director level and help directors keep up to date with the changing regulatory environment, address everyday business challenges as well as promote awareness of best practice and emerging issues. Sessions provide directors with the opportunity to discuss and debate matters with their peers.

Membership of the Deloitte Academy is free to directors of listed companies, and includes access to the Deloitte Academy facilities, a dedicated business centre between Covent Garden and the City. Boardrooms and meeting rooms can be reserved in advance. A lounge area and business desks are available for members to use without prior reservation. Unless otherwise indicated, all briefings are held at the Deloitte Academy facilities.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website **www.deloitteacademy.co.uk** which members can use to register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including membership enquiries, please email **enquiries@deloitteacademy.co.uk.**

### Contacts for the Deloitte Centre for Corporate Governance:

**Tracy Gordon** – 020 7007 3812 or **trgordon@deloitte.co.uk**

**William Touche** – 020 7007 3352 or **wtouche@deloitte.co.uk**

Designed and produced by The Creative Studio at Deloitte, London. J3359