Deloitte.

Cyber risk

Getting the boardroom focus right

- Cyber attacks have become substantially more malicious and larger scale over last few years, causing much greater harm to organisations and elevating cyber risk to principal risk status – requiring reporting under new Corporate Governance Code.
- Digital transformation strategies improve business performance but may also open up organisations to new cyber risks.
- Board members need to establish new governance over cyber risk to ensure that cyber risk is accurately reported to them, that they can direct effective risk management plans, and that they have the expertise to ask the right questions and hold risk owners to account.
- Simply spending more on IT security is not going to solve this, organisations must understand the true impact of attack in order to focus spend effectively.

Organisations have never been more at risk from cyber attacks.

Recent high-profile attacks on companies including retail, media and industrial sectors have highlighted the scale of damage that is now being caused by hackers and cyber terrorists. And this growing threat comes at a time when there is also increasing focus on how organisations manage risk. Regulators, investors and senior executives are putting companies under pressure to explain how they identify risks to their business and how they ensure these are being managed within an agreed risk appetite

The number of security breaches affecting UK businesses decreased slightly in comparison to last year. However, there has been a significant rise in the cost of individual breaches. … 10% of organisations that suffered a breach in the last year were so badly damaged by the attack that they had to change the nature of their business.

2014 Information Security Breaches Survey[1]

Effective governance is a critical aspect of successful risk management: it supports management to execute strategy, manage costs, respond to risk and make better, faster decisions. But as an organisation's risk profile changes, with new risks emerging and the speed and impact with which risks can materialise accelerating, boards need to position themselves, and their governance frameworks, to respond accordingly.

Cyber risk is now central to corporate governance

Significant changes have been made to the requirements for managing and reporting risk. The changes apply to listed companies for accounting periods beginning on or after 1 October 2014. Under the changes to the UK Corporate Governance Code, boards must make a statement confirming they have carried out a robust assessment of the principal risks facing the company, including those that would threaten its business model, future performance, solvency or liquidity. Boards must also describe those risks and explain how they are being managed or mitigated. In addition, the code requires boards to monitor the company's risk management and internal control systems throughout the year. These changes place a direct responsibility on boards to take an active role in assessing and managing risk – and this includes cyber risk.

Nevertheless, there is evidence that many organisations, while being aware of the cyber threat, have not grasped the severity of the risks they face themselves and have not put the governance in place to manage these.

While 88% of respondents from the FTSE350 included cyber risk on their risk register, 75% of boards seldom heard about cyber risk, 24% based their discussions on robust or comprehensive management information, and less than 20% had a clearly set and understood appetite for cyber risk.

Cyber governance health check 2014[2]

1. www.gov.uk/government/ publications/information-security-breaches-survey-2014
2. www.gov.uk/government/ publications/cyber-governance-health-check-2014

Additionally, it appears that many boards overestimate the effectiveness of the mitigation processes they have in place.

> 52% of chief executives believe they have cyber security insurance cover, whereas less than 10% actually do.
>
> HMG/Marsh: UK Cyber Security, March 20153

Cyber attacks cause severe damage to organisations

A critical issue for organisations is to understand that cyber risk is substantially different from IT risk because of the vast amount of damage that can be caused by cyber attack. The 2014 Information Security Breaches Survey defines cyber attacks as "deliberate attempts to cause harm via digital channels".4

Cyber risk has come to dwarf the traditional threats to IT security (or 'information security') as a result of two main changes in the attackers:

- **Objectives:** the UK Government describes cyber attacks as 'malicious'. Attackers are not just looking to steal specific confidential information now. Over the past two to three years there has been a surge in cyber attacks linked to organised crime, nation states and terrorist groups, with the intent to cause large-scale damage to IT systems and to physical systems connected to them.
- **Capabilities:** attackers now have ready access to sophisticated tools and techniques to help them gain access to target IT systems; employees increasingly assist with the attack, either maliciously as 'insiders' or carelessly as unwitting accomplices. The stark reality is that some cyber attacks are not preventable.

The cyber threat is agile and fast changing. Organisations must ensure they are not left behind in the 'arms race' through outdated intelligence on threats and impacts.

The business impact of cyber attacks is developing and growing quickly. Massive volumes of information theft are being reported, with tens of millions of customer records being stolen. Attacks are also focusing on:

- • Changing data and introducing errors into corporate information, e.g. falsifying bank account data to cause fraudulent financial transfers, tampering with process control systems to cause damage to industrial plant.
- • Deleting or encrypting information for harm ('vandalism') or for ransom ('extortion'), e.g. preventing employees from accessing their corporate databases by encrypting the data with unknown keys.
- Crucially, organisations must also recognise that the business may also suffer as a result of cyber attacks that target other companies in their supply chains.

Cyber risk has come to dwarf the traditional threats to IT security as a result of two main changes in the attackers …

3. www.gov.uk/government/ news/cyber-security-insurance-new-steps-to-make-uk-world-centre
4. www.gov.uk/government/ publications/information-security-breaches-survey-2014

What is needed to tackle cyber risk?

Faced with this change in cyber risk and potential impact, boards must now progress from their existing IT risk governance approach and implement effective cyber risk governance. This elevates cyber risk as a principal business risk, collectively owned and managed by the organisation, and not simply a technical risk delegated to the IT department.

Unaware: IT risk governance

Too many organisations still have IT security buried within the IT department. The Chief Information Security Officer (CISO) is left to decide security levels in isolation from the actual business risks he or she is trying to manage, with little access to decision-makers at board level or to adequate funding.

Unaware of the risks, business units frequently perceive IT security simply as a cost and an obstruction and find ways to circumvent it. Similarly, they plan strategy and take business decisions with scant regard for the risk consequences. The lack of board involvement means the regime is not focused and board reporting is inaccurate; the organisation may not be complying with reporting guidelines and impending Financial Reporting Council (FRC) requirements.

Managed: Cyber risk governance

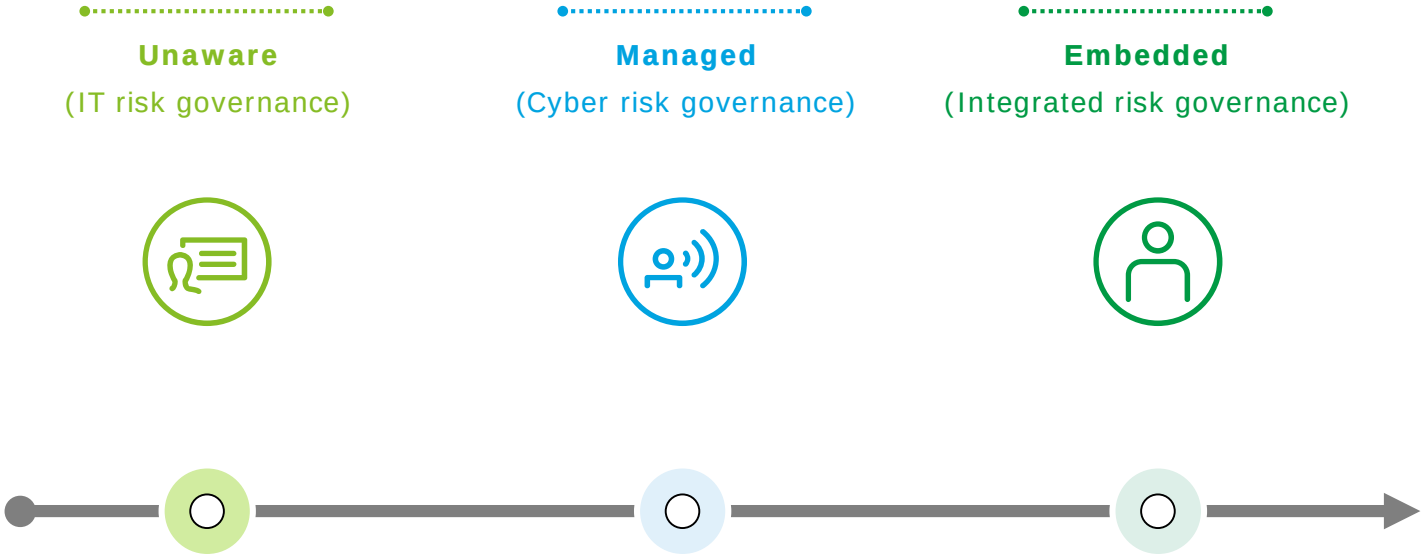
Instead, organisations must implement a new governance process. Board members, senior managers and the CISO, must understand the severity of the cyber threat landscape and how cyber attacks could impact the organisation's finances, business model, customers and reputation. The most damaging impacts need to be identified as priorities for the business and the IT security team: it's not enough to simply increase the security budget, the budget must be focused on the highest priority risks.

It is essential that the appropriate governance is implemented within a structure that suits the individual organisation's corporate governance model, risk appetite and culture, business activities and specific threat landscape.

Embedded: Integrated risk governance

As the organisation improves its ability to manage cyber risk, the cyber governance process will mature and become more embedded in wider risk governance, integrating with related business processes e.g. resilience, business continuity, fraud management and crisis management. The increased maturity of governance will also enable the organisation to introduce more quantitative measurements and to exploit the use of software tools.

Cyber governance maturity



Assurance of the IT security regime

An essential part of cyber risk governance is to enable the board to gain assurance that the IT security regime is fit for purpose, addressing the sophistication of cyber threats and integrating employee security awareness training into the overall regime. This is technically challenging for many boards, external frameworks like the UK Government '10 steps to Cyber Security'5 provide a useful reference, and it may be appropriate to bring in specialist board members or external advisors.

Key indicators for the board

There are some key indicators that you should look out for to see if your board needs to pay more attention to cyber risk:

- Cyber risk is reported by the IT department rather than by business units
- The board has not been made aware of the biggest potential impacts of a cyber attack
- The board has not been briefed at least once in a year about the types of attack that the company faces
- The organisation is planning or undertaking a digital transformation strategy

Characteristics of risk governance at different levels of maturity

Unaware	Managed	Embedded
• The potential impact of cyber attack is not identified or understood by business owners; business decisions are taken without regard for risk. • IT security is implemented within IT department against their internally defined requirements and available budget and is not focused. • Cyber risk appears on Risk Register but the board is not regularly briefed on potential impact and threat, nor provided with appropriate training in cyber. • The board is not able to report accurately on cyber risk and management, and has no crisis management plan for cyber attack.	• Business owners systematically identify cyber risk and impact. • Cyber risk management is established across business, IT and security and defines business requirements for security. • Effective monitoring is implemented to identify threats before attacks complete. • The board is provided with clear management information, enabling decisions on risk appetite and unsustainable events. • The board is briefed regularly on threat and resilience; key board members have high levels of expertise. • The board owns a crisis management plan for cyber attack. • Clear leadership on cyber risk from the board drives a culture change through the organisation.	• Cyber risk management and reporting become 'business as usual', integrated with wider risk portfolio such as business continuity and fraud. • Cyber risk management is increasingly quantified, enabling better assessment and targeting of security spend. • The board is fully aware of internal and external threats, management manages risk proactively in context of threat intelligence and is agile in response to changes in threat. • All board members have up-to-date expertise to participate in cyber discussions. • A crisis management plan is maintained and rehearsed. • All staff recognise their role in supporting cyber risk management

Recent high-profile cyber attacks should be all the incentive boards need to start asking hard-hitting questions …

5. UK Cabinet Office: www. gov.uk/government/ publications/cyber-risk-management-a-board-level-responsibility/10- steps-summary

Deloitte view

- Recent high-profile cyber attacks should be all the incentive boards need to start asking hard-hitting questions on the approach to managing and mitigating the threat of a cyber attack in their organisation; there is no time to waste.
- Boards should make implementing cyber risk governance a priority. They need to ensure they are properly informed and can hold business owners and IT security to account for the identification and management of this major risk to their organisation.
- Boards need to change the organisation's culture from a 'security push' to a 'business pull'.

Contacts

Phill Everson

Lead partner | Cyber risk services

peverson@deloitte.co.uk

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2017 Deloitte LLP. All rights reserved.

Designed and produced by The Creative Studio at Deloitte. CSEDC1616