



BOARD BRIEFING

Cyber Security

Key points

- Cyber security starts with the board and senior management setting a clearly articulated strategy that supports and protects the organisation's objectives.
- A strong cyber awareness culture is one of the best defences against cyber-attacks. Internal audit has a crucial role to play in ensuring that this culture is understood and 'lived' by staff at all levels.
- Forthcoming EU regulations will increase the burden on organisations to ensure they have effective cyber security strategies and culture in place, in addition to robust controls and policies to prevent and remediate attacks.
- The board and internal audit must work together to ensure that all of the organisation's data assets, and the potential cyber threats that could jeopardise those assets, have been adequately mapped out. Cyber assurances agreed in the audit plan should reflect the organisation's cyber risk appetite.

Cyber risk – the board and internal audit

Cyber security has grown to become a key business risk. Technology and data now permeate practically all aspects of business and operations, regardless of sector, from customer data to intellectual property to HR records. This makes virtually all businesses potential cyber-attack targets.

In 2015, Lloyd's, the British insurance market, estimated that cyber-attacks cost businesses as much as \$400bn a year globally and forecast this to rise to as much as \$2trn by 2019. Against this backdrop the UK government announced in its Autumn Statement 2016 a *National Cyber Security Strategy* that will see £1.9bn invested to protect critical infrastructure and raise awareness in the business community.

Accordingly, every UK organisation must prioritise their own cyber strategy. This strategy is the responsibility of the board and the entire executive management team, and the company's defensibility relies wholly on effective cyber governance and controls that support the strategy. Further, forthcoming European

- Union (EU) regulation will place greater demands on businesses, their boards and management to embed effective cyber strategies.

Internal audit has a critical role to play in assuring that cyber security risk controls, policies, and procedures are fit for purpose and being implemented effectively at all levels. *The IIA Global Technology Audit Guide, Assessing Cyber Security Risk: Roles of the Three Lines of Defence*, is an essential tool for internal auditors working in this area.

A new era of regulation

The transposition of the *Network and Information Security (NIS) Directive* and *General Data Protection Regulation (GDPR)* represents the EU's most significant cyber initiative. Despite the UK Government's plans to leave the EU, it has indicated that it intends to transpose all existing EU legislation into domestic law, meaning all regulation will remain in force until the current or future UK Government legislates to change them. Moreover, any businesses offering any type of service to the EU market, regardless of whether they store or process data on EU soil, will be bound by the rules.

The immediate impact of the implementation of the NIS Directive will be to draw into regulatory scrutiny many organisations deemed to be ‘operators of essential services’ that may have previously lain beyond the scope of existing cyber security legislation (see boxes).

For the most part this will require a risk-based approach of taking “appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.” The NIS Directive also requires that any breaches that seriously compromise operators’ networks are reported to a designated authority – namely the Computer Security Incident Response Teams that each member state is required to establish.

The GDPR will add another layer of regulation that, for the purposes of cyber security, chiefly relate to the security of personal data. These additional rules will also introduce significant financial penalties for companies found to have failed in keeping personal data appropriately secure (see box).

This incoming regulation has implications for internal audit functions and the work they carry out in helping to manage cyber risk and defend organisations from attack. It is crucial for the board and the audit committee to give internal audit a clear mandate around cyber security, and to write that mandate formally into the audit charter of the organisation.

Board, audit committee and senior management recommendations

- The board should work with executive management to set a clear organisational cyber strategy, understand how that strategy supports the organisation’s objectives, and seek assurance that staff at all levels understand the strategy and how it protects the organisation.
- Executive management should proactively ensure the organisation is resilient against cyber-attacks, rather than waiting for an attack to occur and reacting when it happens. Internal audit can provide assurance to the board that proactive policies and measures are in place and working.
- Both the board and senior management should be aware of key risks related to cyber security and their likely impact, and the board must be confident that management has performed a risk assessment to identify assets susceptible to cyber threats or security breaches.
- The board/audit committee should work with the chief audit executive (CAE) to ensure that cyber audit plans are comprehensive and reflect the organisation’s risk appetite and objectives.

- Senior management and the board should be aware of forthcoming EU regulations, how they will affect the organisation, and take any necessary steps to ensure compliance. The board should also consider including cyber regulatory compliance in future audit plans.
- The board/audit committee and CAE should be confident that the internal function has the skills and resources necessary to provide assurance on cyber security, and agree to co-source expertise where needed.
- Boards should try to embed a strong culture of cyber awareness and best practice. Careless employee behaviour can result in cyber breaches, so periodic awareness training and assurance that staff fully understand cyber security policies and procedures are essential.
- Technology and cyber security are incredibly fast moving. Accordingly, the internal audit function should include auditors with the requisite knowledge of technology and security frameworks to understand whether cyber risk is being effectively managed. The function should also routinely engage with internal and external subject matter experts to understand the changing nature of the threat and, in most cases, co-source expertise to run comprehensive cyber audits.
- Embedding a company-wide culture around cyber security that is ‘lived’ and manifests itself in staff behaviour, rather than simply being understood, is essential. Too often, organisations focus on implementing technical measures in response to cyber security risk over an organisational response. Internal audit can play a significant role in this organisational response by providing assurance over cyber risk awareness and whether the overarching cyber strategy is reflected in employee behaviour and effective controls.

In conclusion

As it stands, a gap exists between the scale of the cyber threat and efforts being made to address the threat. The Government’s recent *Cyber Security Breaches Survey 2016* found that whilst 69% of businesses say their senior management consider cyber security to be a very or fairly high priority for their organisation, only half of businesses have actually taken recommended actions to identify cyber risks. It is time to close that gap.

With the cost of cyber-attacks and security breaches escalating, boards must ensure they are doing everything they can to protect their organisations. This requires working with senior management to formulate a clear cyber strategy and utilising internal audit to determine how effectively cyber risks are being managed.

Incoming data regulation in a nutshell

The Network and Information Security (NIS) Directive

The NIS Directive applies to ‘operators of essential services’ in both the private and public sectors. The first step for all organisations is to determine whether they fall under the scope of the Directive, which covers energy, transport, banking and financial market infrastructures, health, water, elements of public administration, and certain digital service providers.

Regulated operators will have to take appropriate security measures that include:

- Preventing risks: technical and organisational measures that are appropriate and proportionate to the risk
- Ensuring security of network and information systems: the measures should ensure a level of security of network and information systems appropriate to the risks
- Handling incidents: the measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

‘Serious incidents’ should be reported to the relevant national authority that member states will be required to establish to conform to the Directive. The regulation does not define a threshold for what constitutes a serious incident; however, the following three parameters should be taken into consideration: number of users affected, duration of incident, geographic spread.

The Directive is to be transposed to UK law by April 2018 and operators of essential services are to be identified within the following six months.

An English version of the full Directive can be found here: bit.ly/NISdirective

The General Data Protection Regulation (GDPR)

The GDPR has a potentially wider reach than the NIS Directive as it applies to all organisations’ secure management of personal data. In many respects it will mirror the UK’s existing *Data Protection Act* (DPA), although, importantly, will feature a broader definition of what constitutes personal data; it’s safe to say that companies currently abiding by the DPA will have to obey the GDPR.

The regulation will require organisations of over 250 employees to appoint a data protection officer.

Companies found to have breached the requirements of the regulation once the transposition period has concluded may face significant fines.

Administrative and security breaches will attract a lower-tier fine of up to €10m or 2% of global turnover, whichever is greater.

Where data subjects’ rights and freedoms are seen to have been infringed, however, a higher-tier fine of up to €20m or 4% of global turnover, whichever is greater, may be imposed.

Organisations will need to be compliant when GDPR comes into effect in May 2018.

An English version of the full Directive can be found here: bit.ly/GenDPR

About the Chartered Institute of Internal Auditors

First established in 1948, the Chartered Institute of Internal Auditors (Chartered IIA) obtained its Royal Charter in 2010. It is the only professional body dedicated exclusively to training, supporting and representing internal auditors in the UK and Ireland. It has over 9,000 members in all sectors of the economy including private companies, government departments, utilities, voluntary sector organisations, local authorities and public service organisations such as the National Health Service.

Over 2,000 members of the institute are Chartered Internal Auditors and have earned the designation CMIIA. Over 800 of our members hold the position of head of internal audit and the majority of FTSE 100 companies are represented amongst the institute's membership.

Members of the Chartered Institute of Internal Auditors are part of a global network of over 180,000 members in 170 countries. All members across the globe work to the same International Standards and Code of Ethics.

More information on the Chartered IIA is available at www.iaa.org.uk

www.iaa.org.uk

Chartered Institute
of Internal Auditors

13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

tel 020 7498 0101

fax 020 7978 2492

email info@iaa.org.uk

© March 2017