CYBER AND DATA SECURITY
PERSONAL LIABILITY FOR C-SUITE EXECUTIVES

Aravind Swaminathan and Adele Harrison of Orrick, Herrington & Sutcliffe LLP examine when C-suite executive leaders may be held individually accountable for cyber security and data protection incidents.

Cyber security and data protection issues continue to occupy an important place within corporate governance. At the same time, there is an increasing trend towards individual culpability for senior managers and C-suite executives across many regulatory areas. Businesses and their leaders should expect this trend increasingly to extend to cyber security and data protection matters. This personal accountability serves to reinforce the significance of these issues and highlights that C-suite executives must maintain a vigilant and proactive stance.

This article discusses:

- C-suite liability for cyber incidents, exploring both the direct responsibilities of C-suite executives to prevent cyber breaches and the legal repercussions that they face in the event of a cyber incident occurring.
- The potential personal liabilities under the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR).
- The roles of the Financial Conduct Authority (FCA) and the UK Corporate Governance Code (the Code), which highlight the critical need for robust cyber security measures and prudent risk management.
- The impact of the Network and Information Security (NIS) II Directive (*2022/2555/EU*) (*see box "NIS II Directive"*).
- The steps that C-suite executives can take to minimise their risk of liability.

The term "C-suite" refers to the executive-level managers within an organisation, including the CEO, the chief financial officer, the chief operating officer, the chief information officer (CIO) and the chief information security officer (CISO).

CYBER INCIDENTS

The senior leaders that make up the C-suite often become a focal point for both claimants and regulators in the aftermath of a cyber incident, as these executives are responsible for setting and implementing (or, at a minimum, supervising those who set and implement) an organisation's cyber security priorities and cyber security strategies in order to ensure that the organisation is adequately protected.

Claimants and regulators may target the C-suite in order to ensure accountability and to act as a deterrent for failing to carry out their duties (*see box "US trends"*). This

personal accountability emphasises the importance of executive responsibility in safeguarding against cyber risks which, in turn, drives more effective cyber security measures within organisations.

Generally, in the UK, directors can be held liable for breaches of their statutory fiduciary duties and, in some circumstances, negligence and other torts. Directors can be liable or jointly liable for tortious acts where they are directly involved in the wrongful activity (*www.practicallaw.com/5-206-5011*). These torts could include the misuse of private information, breach of confidence and negligence.

Corporate liability

Under the UK GDPR, businesses have an obligation to notify the UK's data protection regulator, the Information Commissioner's Office (ICO), after certain cyber incidents that involve personal data breaches which result in a risk to the rights and freedoms of natural persons (*Article 33(1)*). A notification to the ICO can make subsequent regulatory action more likely.

Regulators such as the ICO typically carry out investigations into breaches notified to them. This usually involves submitting follow-up questions to the notifying organisation regarding details of the breach, such as the controls and protections in place, the number of data subjects affected or how the threat actors gained access to and traversed affected systems.

The main liability risks to businesses of receiving an ICO penalty, such as a fine or enforcement notice, are:

- Financial risk, for example, under the UK GDPR, failing to notify a breach when required to do so can result in administrative fines of up to £8.7 million or 2% of annual global turnover.
- Reputational risk, as a public enforcement notice issued by the ICO under the UK GDPR will be published online and will likely contain details of the business's security and organisational failures to prevent the attack.
- Legal risk, as a public enforcement notice issued by the ICO can provide potential claimants with important information that could assist them in bringing actions against the business to claim compensation for an infringement of the UK GDPR. Individually, these may be small claims but, when aggregated at scale, they can be challenging for organisations to address in the aftermath of a breach.

In addition to these risks that the business may face, individuals may also be liable under the UK GDPR (*see "UK GDPR" below*).

Directors' fiduciary duties

Directors are subject to statutory duties under sections 171 to 177 of the 2006 Act, which are based on certain common law rules and equitable principles. The duties are owed to the company and not to the shareholders. The two duties that are especially relevant to the prevention of cyber incidents are:

- The duty to promote the success of the company, including having regard to a long-term view, the interests of employees and the desirability of the company to maintain a reputation for high standards of business conduct (*section 172, 2006 Act*) (section 172).
- The duty to exercise reasonable care, skill and diligence, which takes into account the general knowledge, skill and experience that may be reasonably expected of a person carrying out the functions of that director in relation to the company, and the general knowledge, skill and experience of the director themself (*section 174, 2006 Act*) (section 174).

Section 172 duty. If a business implements insufficient or inadequate cyber security controls, this could amount to a failure by the directors to consider the likely long-term consequences of decisions and the desirability of the company to maintain a reputation for high standards of business conduct, as required by section 172.

Effective cyber security demands a long-term view. Misplaced short-term monetary and human resource savings in this area

NIS II Directive

From 18 October 2024, the Network and Information Security (NIS) Directive (*2016/1148/EU*) was repealed and replaced by the NIS II Directive (*2022/2555/EU*). The NIS II Directive is intended to address cyber security requirements throughout EU member states and it could expand personal and corporate liability. It expressly addresses governance requirements, including requiring that the management body must approve the cyber security risk-management measures taken by the entity and oversee their implementation. Member state law implementing the NIS II Directive must ensure that the management is held liable for infringements by the entity (*Article 20(1)*).

Member states had until 17 October 2024 to adopt and publish the measures necessary to comply with the NIS II Directive and were required to apply them from 18 October 2024. As yet, it is too early to get a full picture on how these C-suite liability requirements will be transposed into the national laws of member states.

The NIS II Directive will only apply in the EU but it is possible that the UK will, in due course, adopt a similar approach. The current regulation in the UK is contained in the NIS Regulations 2018 (*SI 2018/506*) (2018 Regulations), which implemented the now superseded NIS Directive (*see Briefing "Network and Information Systems Regulations: assessing the impact", www.practicallaw.com/w-018-7097*).

In November 2022, the previous government published proposals for reforming the 2018 Regulations (*www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/f024001d-62c1-48b5-873a-64d240d73f1f; see Briefing "Extended cyber security requirements: the picture in the EU and the UK", www.practicallaw.com/w-039-2445*).

In the King's Speech on 17 July 2024, the new government set out a Cyber Security and Resilience Bill, with proposals that appear similar to those planned by the previous government but there is, as yet, no detail on the contents of the Bill (*see News brief "King's Speech 2024: all change?", www.practicallaw.com/w-043-9124*).

can have negative consequences in the long term when an organisation is hit with a cyber attack. These include financial, reputational, legal and organisational repercussions. In relation to the company's reputation, a cyber attack, especially one that involves either highly sensitive commercial information or personal data, can have a damaging effect on an organisation's standing. Directors must therefore act with this in mind when making decisions on investing in, and dedicating resources to, cyber security.

Directors must also pay heed to the interests of the company's employees under section 172 (*see feature article "Cyber incidents: managing the employee fallout", www.practicallaw.com/w-035-0663*). Companies have to collect personal data relating to their staff such as contact details, bank details and home addresses. A company that fails to adequately protect this personal data will be at greater risk of a damaging data breach and may also be liable to aggrieved employees under data protection regimes.

In order to discharge their duties to employees under section 172, directors must make sure that employee data is adequately protected. The ICO's draft guidance on employment practices and data protection is a helpful resource that sets out good practice to help employers comply with data protection legislation (*https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/keeping-employment-records/*).

Section 174 duty. It is critical for company directors to ensure the selection and implementation of adequate cyber security measures that are proportionate to the company's risk profile. A failure to do so could constitute a breach of the section 174 duty.

Directors' responsibilities include the appointment of appropriately staffed teams with the requisite expertise as well as the installation of adequate hardware and software. In addition, executives appointed as a CIO or CISO, who are likely to have a background in IT or a related field, are held to an elevated standard. This is because the general knowledge, skill and experience that the individual director has is a factor in assessing whether there has been a breach of the section 174 duty.

Each director therefore needs to acquire a general understanding of the cyber security risks that the company faces, if they do not already possess this understanding. They must also maintain an up-to-date understanding of the risks, be aware of current cyber security issues and take expert advice where required.

Directors may face scrutiny and accountability if their actions or inaction lead to a breach of the section 174 duty in overseeing the company's cyber risk management.

US trends

In the US, there has been an increase in the targeting of regulatory or other legal action at senior individuals in organisations as a result of high-profile cyber incidents and data breaches. For example, in October 2023, the US Securities and Exchange Commission sought to hold the chief information security officer (CISO) of SolarWinds Corp personally liable for the Russian hack that compromised the company's systems in 2020, although most of the charges were eventually dismissed (*www.reuters.com/legal/us-sues-solarwinds-court-records-2023-10-30/*).

In 2023, the former CISO of Uber Technologies Inc was the first company executive to be criminally prosecuted over how they handled a data breach (*www.bbc.co.uk/news/technology-65497186*). There is also an increase in publicity around these matters, which often includes naming the relevant individuals at the affected organisation. It may be that these trends will be replicated in other parts of the world, including in the UK.

Consequences of a breach

The company, acting through the board of directors, can bring a civil action against a director in respect of a breach or breaches of the general statutory duties in the 2006 Act. While the 2006 Act does not codify the civil consequences of a breach, section 178 states that:

- The consequences of a breach or threatened breach of sections 171 to 177 of the 2006 Act are the same as would apply if the corresponding common law rule or equitable principle applied.
- The duties in those sections, with the exception of the section 174 duty to exercise reasonable care, skill and diligence, are enforceable in the same way as any other fiduciary duty owed to a company by its directors.

Consequently, the company has a range of potential remedies against a director for a breach of their duty, including:

- An account of profits.
- The restoration of property or profits.
- Injunctive relief to prevent a breach or a continuation of a breach.
- The rescission of a contract entered into by the director.
- Damages, which may be damages in equity, which are potentially wider in scope than the usual compensatory measure.

However, the duty to exercise reasonable care, skill and diligence under section 174 is not considered to be a fiduciary duty. It is, in effect, a claim that a director has acted negligently, so the usual remedy will therefore be compensation for the loss suffered as a result of the director's conduct by way of damages. Generally, the proper person to bring a claim is the company, acting through the board, because the duties are owed to the company, not to any individual.

However, other persons may be able to bring certain types of claims based on a breach of the general duties in some circumstances as described below.

Derivative claims. Shareholders may bring a derivative claim on behalf of the company under sections 260 to 264 of the 2006 Act (*see Focus "Statutory derivative claim regime: ten years on", www.practicallaw.com/w-008-7613*). A derivative claim may be brought in respect of a cause of action arising from an actual or proposed act or omission involving negligence, default, breach of duty or breach of trust by a director of the company. The claim is derived from the rights of the company. The bar for this kind of claim is high, as demonstrated by the recent

decision in *ClientEarth v Shell plc*, where the High Court refused to grant permission for a derivative action based on the directors' alleged failures to take sufficient action to address climate change or reduce emissions (*[2023] EWHC 1897 (Ch), www.practicallaw.com/w-040-4924; see feature article "ESG claims against directors: contending with the changing climate", www.practicallaw.com/w-040-9447*). It is unlikely that these types of claims will arise routinely in respect of cyber security incidents.

Unfair prejudice. Breaches of the directors' duties are often relevant in the context of cyber incidents because they may form a basis for unfair prejudice (*see Briefing "Unfair prejudice petitions: flexibility and creativity", www.practicallaw.com/w-022-9655*). Minority shareholders may seek relief from the court by way of an unfair prejudice petition under sections 994 to 999 of the 2006 Act if they believe that the affairs of the company have been, are being or will be conducted in a way that is unfairly prejudicial to the members in general or the petitioner specifically. The normal remedy is a share purchase order.

Misfeasance. In an insolvency situation, the liquidators of a company could potentially bring a misfeasance claim under section 212 of the Insolvency Act 1986. This provides a route for a claim against certain persons, including officers of the company. It applies where, in the course of the winding up of a company, it appears that the person in question has misapplied or retained, or become accountable for, any money or other property of the company, or been guilty of any misfeasance or breach of any fiduciary or other duty in relation to the company.

The courts have traditionally allowed company directors some flexibility and discretion to decide how they comply with their duties. For instance, in *ClientEarth*, the court affirmed the well-established principle under English law that it is for the directors themselves to determine, acting in good faith, how best to fulfil the section 172 duty to promote the success of the company for the benefit of its members as a whole. The court also refused to impose overly prescriptive obligations on the directors in respect of their section 174 duty.

In relation to cyber security and data protection compliance, a lack of controls, or clearly inadequate controls or compliance programmes, could potentially be serious enough to be a breach of this duty despite the wide discretion given to directors to manage the company's affairs as they see fit.

Disqualification. Directors may also be disqualified by a court under section 6 of the Company Director Disqualification Act 1986 if it is found that they are unfit to be concerned in the management of a company. This could be the case if they have failed to implement adequate cyber security measures or to adhere to the necessary data protection principles.

Service contracts. Aside from statutory penalties, directors in breach of their duties will also likely be in breach of their service contracts with the company, which will normally give the company a right to terminate the contract.

UK GDPR

Individuals, including sole traders, partners in unincorporated partnerships, and self-employed professionals, can be data controllers. Outside of these categories, it is less likely that C-suite executives, as opposed to the business, would be identified as the controller. Liability for individuals can arise for breaches of the Data Protection Act 2018 (DPA 2018). Individuals can be prosecuted by the ICO for the criminal offences of:

- Knowingly or recklessly obtaining or disclosing personal data without the consent of the controller (*section 170, DPA 2018*).
- Knowingly or recklessly re-identifying information that was previously de-identified (*section 170, DPA 2018*).
- Altering or concealing information that should have been provided in response to a data subject access request (*section 173, DPA 2018*).

A conviction for one of these offences can lead to an unlimited fine.

Section 198 of the DPA 2018 permits directors to be found guilty of the relevant offence and liable to prosecution, as well as the body corporate, where a criminal offence under the DPA 2018 is committed with their consent or connivance.

FCA REGULATION

The FCA, in its role as the regulator of financial services firms, is increasingly aware of cyber security incidents affecting regulated firms. This is highlighted by its publication of a report bringing together industry insights on cyber resilience security, which was published on 8 March 2019, and the introduction of cyber co-ordination groups that, together with industry stakeholders, seek to improve cyber security practices (*www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf*).

The FCA Handbook addresses systems and controls, and risk control, in the Senior Management Arrangements, Systems and Controls sourcebook (SYSC). A regulated firm must take reasonable care to establish and maintain the systems and controls that are appropriate to its business, which include cyber security measures (*SYSC 3*). A firm must have in place effective processes to identify, manage, monitor and report the risks that it is, or might be, exposed to (*SYSC 7*).

The Financial Services and Markets Act 2000 provides the requisite authority to create the rules in SYSC that form part of the FCA's regime to regulate financial services firms. The FCA's disciplinary and enforcement tools for a regulated firm range from public censure to the cancellation of an authorised firm's permission to conduct regulated activities and the imposition of fines (*see feature article "New UK regulatory landscape: enforcement and supervision shift", this issue*). These enforcement tools are detailed in Chapter 7 of the FCA Handbook.

The FCA has confirmed that it will not discipline individuals on the basis of vicarious liability; for example, it will not hold them responsible for the acts of others, provided that appropriate delegation and supervision has taken place (*Decision Procedure and Penalties manual 6.2.7, FCA Handbook*) (DEPP 6.2.7).

The FCA has also confirmed that disciplinary action will not be taken against an approved person performing a significant influence function (SIF) or a senior conduct rules staff member simply because a regulatory failure has occurred in an area of business for which they are responsible (*DEPP 6.2.7*). Broadly, a senior conduct rules staff member is a person who carries out senior management functions at a firm that is subject to the senior

managers and certification regime or is a non-executive director (*see Briefing "Senior managers and certification regime: another year on", www.practicallaw.com/w-013-8923*).

The FCA will consider that an approved person performing a SIF may have breached certain Statements of Principle, or that a senior conduct rules staff member may have breached certain rules, only if their conduct was below the standard that would be reasonable in all of the circumstances at the time of the relevant conduct. C-suite executives should therefore ensure both the appropriate delegation of responsibility, and the supervision of cyber security measures and data protection programmes, and that their conduct in these areas meets the expected standard.

While the FCA may be reluctant to pursue individuals, on 19 February 2019, it entered into a memorandum of understanding with the ICO where the two organisations agreed to co-operate, stating that they will alert each other to any potential breaches of the legislation regulated by the ICO, within the context of this relationship, that was discovered while undertaking regulatory duties, and will provide relevant and necessary supporting information (*www.fca.org.uk/publication/mou/mou-fca-ico.pdf*). This is likely to mean that for businesses regulated by the FCA, any potential data protection issues can be flagged to the ICO, leading to exposure to the ICO's enforcement powers.

CORPORATE GOVERNANCE

The Code applies to public companies with a premium listing and, while it is not legally binding, it is a powerful tool that provides principles and provisions of good practice (*see feature article "UK Corporate Governance Code: living in a material controls world", www.practicallaw.com/w-043-2524*). Provisions 28 and 29 of the Code (provision 28) (provision 29) deal with the company board's approach to risk management.

Under provision 28, the board directors are required to confirm in the annual report that they have completed a robust assessment of the company's emerging and principal risks, as well as the procedures that are in place to identify emerging risks and how these risks are managed or mitigated. In the current climate, cyber risks are emergent, if not already existing, risks for most companies and should therefore be addressed in the annual report. Amid the growing cyber threat landscape, it is also increasingly likely that investors will expect a public company to have in place adequate strategies to deal with these risks.

Provision 29 requires boards to monitor the company's risk management and internal control systems and carry out, at a minimum, an annual review of their effectiveness, which should also be included in the annual report. To enable this assessment to be carried out, it is critical that directors have a sufficient understanding of cyber risks to appreciate the required management and mitigation strategies and their respective effectiveness.

A new section in the Financial Reporting Council's guidance on the Code (the guidance), which was updated on 4 December 2024, discusses the crucial role

Related information

This article is at practicallaw.com/w-044-6910

Other links from uk.practicallaw.com/

Topics

Compliance: data protection	topic/1-616-6178
Corporate governance	topic/8-103-1148
Data, information and cyber security: practice compliance	topic/w-033-2270
Data protection: general	topic/1-616-6550
Data security	topic/8-616-6189
Directors	topic/7-200-0622
Identify and assess risk	topic/w-033-2278
Information technology	topic/5-103-2074
Internet	topic/8-383-8686

Practice notes

Cyber insurance: an overview	w-026-4193
Cyber security: FCA regulation	w-025-6041
Data breach notification (UK)	w-013-5105
Data security under the UK GDPR and DPA 2018	w-013-5138
Derivative claims	8-546-6725
Directors' duties: directors' general duties under the Companies Act 2006	7-376-4884
Maintaining a transparent and constructive relationship with the Information Commissioner's Office (ICO)	w-013-0770
Managing cybersecurity risk and compliance	6-615-8326
NIS 2 Directive: overview	w-037-2098
Overview of cybersecurity	9-617-7682
Security incident notification requirements (UK)	9-616-4019

Previous articles

FCA and PRA enforcement in 2023: a shake-up (2024)	w-041-8915
Smart products and devices: new cybersecurity rules for the UK (2024)	w-043-6464
UK Corporate Governance Code: living in a material controls world (2024)	w-043-2524
Cyber incidents: managing the employee fallout (2022)	w-035-0663
Changing face of cyber insurance: the devil finds work for idle hands (2021)	w-031-9892
GDPR enforcement: a changed landscape (2021)	w-030-5470
Cyber risk and directors' liabilities: an international perspective (2016)	2-635-5748
Cyber security: top ten tips for businesses (2016)	3-621-9152
Cyber security: litigation risk and liability (2014)	1-568-4185

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

of the board in cyber security, with a focus on ensuring operational resilience and the continuous functioning of the business (*www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance/*). The guidance states that directors should have enough knowledge for constructive discussions with key personnel to be confident that cyber risk is being managed appropriately as part of the company's general organisational risk management.

MINIMISING RISK

C-suite executives can take certain steps to minimise their personal liability for cyber security and data protection incidents.

Compliance programmes

As with all enterprise risks, the key to managing the risk of cyber attacks is to have a comprehensive compliance programme (*see feature article "Cyber security: top ten tips for businesses", www.practicallaw.com/3-621-9152*). The parameters of a compliance programme are beyond the scope of this article, but it is important to note, in particular, that the compliance effort for cyber threats should be co-ordinated between the legal, IT and IT security teams.

Compliance programmes will necessarily be complicated, and will differ by a host of factors, including the type of organisation, the industry sector, geographical location and the nature of the business but many elements are likely to be common, such as business-wide cyber security training, good password practice, technology solutions to alert to security incidents and events quickly, and sophisticated backups, just to name a few. Testing incident response capabilities, processes and teams is particularly important, especially through tabletop exercises that can help organisations to better understand and manage the risks.

The National Cyber Security Centre (NCSC) publishes useful toolkits, advice and guidance for businesses of various sizes (*www.ncsc.gov.uk/section/advice-guidance/all-topics*). Directors may find it useful to refer to the NCSC's comprehensive toolkit for directors (*www.ncsc.gov.uk/collection/board-toolkit/cyber-security-regulation-and-directors-duties-in-the-uk*).

A good data protection compliance programme is essential. If a data breach occurs, the impact can be limited where appropriate data retention, data security and deletion policies are in place and enforced (*see Focus "Data protection training and compliance: when DPOs become teachers", www.practicallaw.com/w-026-1255*).

Board reporting

In order to protect against allegations that the board has somehow failed in its duties in respect of cyber security risks, it is important for the board to receive regular and relatively detailed reporting from relevant advisers. As a significant and developing enterprise risk, cyber security should be a standing agenda item. Boards should take the time to become familiar with the issues and ask questions of their teams to understand the business's position. Issues should be escalated and the follow-up on any outstanding items should be addressed at subsequent meetings.

Exclusion or limitation of liability

Any attempt to include a provision in a company's articles or in a contract that exempts a director from any liability that would otherwise attach to them in connection with negligence, default, breach of duty or breach of trust in relation to the company is void (*section 232, 2006 Act*).

Section 232 of the 2006 Act also voids any provision that directly or indirectly provides an indemnity for a director of the company or an associated company against any liability attaching to them in connection with any negligence, default, breach of duty or breach of trust in relation to the company of which they are a director, except as permitted by:

- A provision of insurance.
- A qualifying third-party indemnity provision.
- A qualifying pension scheme indemnity provision (*section 232(2), 2006 Act*).

Aravind Swaminathan is a partner, and Adele Harrison is a senior associate, at Orrick, Herrington & Sutcliffe LLP.

