“A lack of personal responsibility has been commonplace throughout the industry,” said UK MP Andrew Tyrie, who is the chairman of the UK’s Parliamentary Commission on Banking Standards, upon release of the commission’s report ‘Changing Banking for Good’ in June 2013. “Senior figures have continued to shelter behind an accountability firewall,” he added.

Individual and collective responsibility at senior management and board level is being codified to address this ‘lack’. On March 7, 2016, the Senior Managers Regime (SMR) will come into effect in the UK. It will ask that banks, building societies, credit unions and certain firms designated by the Prudential Regulatory Authority (PRA) – typically large investment banks and branches of foreign banks – are able to identify who specifically is responsible for areas of the business, with written responsibilities and a map put in place to formally link these up.

Any staff who take material risk or are considered to pose a risk of significant harm to the firm or customers (for example, as advisors) must be identified by the time the regime comes into effect and be certified for their role within the following 12 months.

TAKING RESPONSIBILITY
Michael Ruck, senior associate at law firm Pinsent Masons, says: “[The authorities] want to see increased transparency within firms, and they want [firms] to almost stop and think carefully about who should be responsible, who is the best person, the appropriate person, for example, whether that be the person most experienced in the relevant roles, as to where that responsibility should fall. When they walk through the door, they know exactly who is responsible for what.”

Within financial institutions, the ‘three lines of defence’ model has traditionally been used to deliver risk governance. The model outlines: a primary function that owns and manages risk; a secondary specialist supervisory risk management and/or compliance function; and a tertiary function that provides independent oversight and internal audit functions.

Patricia Jackson, risk governance leader at consultancy EY, says that the application of this model has become skewed. This will affect the way firms can react to an imposed model of risk governance, in particular increased individual accountability.

‘A question that arises is whether individuals have the wherewithal to discharge the responsibility,’ she says. “That dovetails with thinking globally that the way the three lines of defence model has been applied has put increasing focus on the second-line control functions at the expense of ownership of risk on the frontline. That was a very damaging outcome. The role of the second line cannot be weakened, and in fact must be strengthened, but you have to have ownership of all risk – including behaviour – in the frontline.”

Where risk can be defined and quantified, ownership is possible. A new and ill-defined area creates a challenge even for firms applying the three-line model effectively; cyber risk management. In the context of the SMR, this is a hot potato.

THE GREATEST RISK
The “accountability firewall” that Mr Tyrie referred to has proven more resilient than the electronic firewalls that are used to defend firms from cyber attack. From JPMorgan to Nasdaq, major financial institutions have fallen victim to electronic infiltration, bombardment or both. Tackling this amorphous threat is enormously complicated. For individual firms, calculating the potential losses and risks that they are exposed to is a real challenge. Theft of intellectual property does not require the removal of the property but the copying of it. Breaking into a firm does not require any damage to be caused. Intruders can exist within a firm’s technology infrastructure for years. The intruders could be
foreign government agents breaking in via the internet or staff members.

Investors are voicing concern about the awareness that boards and senior management have of the threat. Legal & General Investment Management (LGIM) has called for action from the government and major investors together with the introduction of compulsory cyber audits, citing cyber security as “a significant risk to our investee companies.”

Ken Allan, global information security leader at EY, says that in the eyes of stakeholders, the issue has moved from the realm of IT to the realm of risk governance. “If you presided over a major breach, there are often questions to be asked; they are no longer in the realm of ‘why were you breached?’ they are more in the realm of ‘what did you do to prepare for it?’,” he observes.

Sarbjit Nahal, equity strategist at Bank of America Merrill Lynch, notes that 35% of companies say cyber risk is not on the board-level agenda and he believes that it should be. That will require board members who have knowledge not only of technology but of cyber security. “We see more companies hiring people with knowledge of this topic, able to provide independent oversight over this,” says Mr Nahal. “Where does this function sit? Is it board level? Does it end at a chief security officer?”

This is crucial if a firm is to get a perspective on the risk that reflects its impact on the whole business rather than the IT team, warns Mr Allan. “The loss of service on a rack of servers bears no relation to three years of research into a brand new drug that [the company] has been planning to bring to market,” he says. “IT people in general don’t understand that.”

**CYBER RISK GOVERNANCE**

Faced with a new regime for accountability and a poorly understood threat, boards must have a demonstrable plan for approaching the problem that can appease stakeholders and regulators.

In Consultation Paper CP 18/15 published in May, the PRA said that while “even a broadly constituted and well-experienced board cannot necessarily be expected to have expertise in every aspect of a broad and complex financial business”, it ought to have “the diversity of experience and capacity to provide an effective challenge across the full range of the firm’s business and the opportunity to explore key business issues rigorously”.

Ms Jackson says that although boards are not in the same position as senior management when it comes to knowing or understanding all of the risks to which a firm is exposed, that does not mean they will avoid the burden of that risk management.

“Boards will never know all of the risks being conducted in the firm, they can’t be as close to it as senior management. It would be inappropriate for them to be. They don’t run the day-to-day business,” she says. “The PRA tried to clarify that earlier in 2015 when it issued a paper saying, for example, that the chair of the risk committee is responsible for the governance of the risk committee and the way that information flows to it, but board members are still very fearful that regulators expect them to manage the risk in a way that is not possible or appropriate.”

David Patt, senior analyst for corporate governance and public policy at LGIM, argues that investors do not expect the board to understand day-to-day IT operations, or to offer a guarantee, but they do expect the board to be dealing with this risk at a strategic level.

“Breaches do happen, however if it were the case that a firm had not prepared itself for a breach, with the board failing to implement best practice and keep itself informed, then it would have to answer to investors for that,” he says. “Risk culture comes from the top.”

**REMOVING THE MYSTERY**

To successfully manage the position in which it finds itself, the board of directors will first need to engage itself in discussion of the issue and start to remove the mystery surrounding it.

Ms Jackson says: “The board has to ask if it is getting the right information to work out if the bank has taken a wrong turn or if the strategy is taking it into a high-risk area. The risk appetite discussion is hugely helpful: asking how much loss they want to take, or can they take, really crystallises the matter.”

Formalising the approach to managing this risk in such a way that satisfies the SMR but goes beyond a box-ticking exercise will require a rethinking of the three lines of defence model to specifically deal with cyber security, says Mr Allan. The first line of defence would be policies and user education and people understanding their responsibilities, and the second line of defence would require a highly sophisticated monitoring capability to track the vast activity within the firm while looking for anomalies in the data.

“My third line of defence is going to be the act of looking outside the organisation,” adds Mr Allan. “Who might be attacking me? What do they have to gain by doing that? What intelligence can I gather to try to defend against it? So it’s not three lines of defence as the head of internal audit would think about it, it’s three lines of defence on a completely different scale.”

**Bit of a tangle: the Senior Managers Regime requires firms to identify the individuals responsible for specific areas, but the question of who is responsible for cyber risk management is causing problems within this new model**