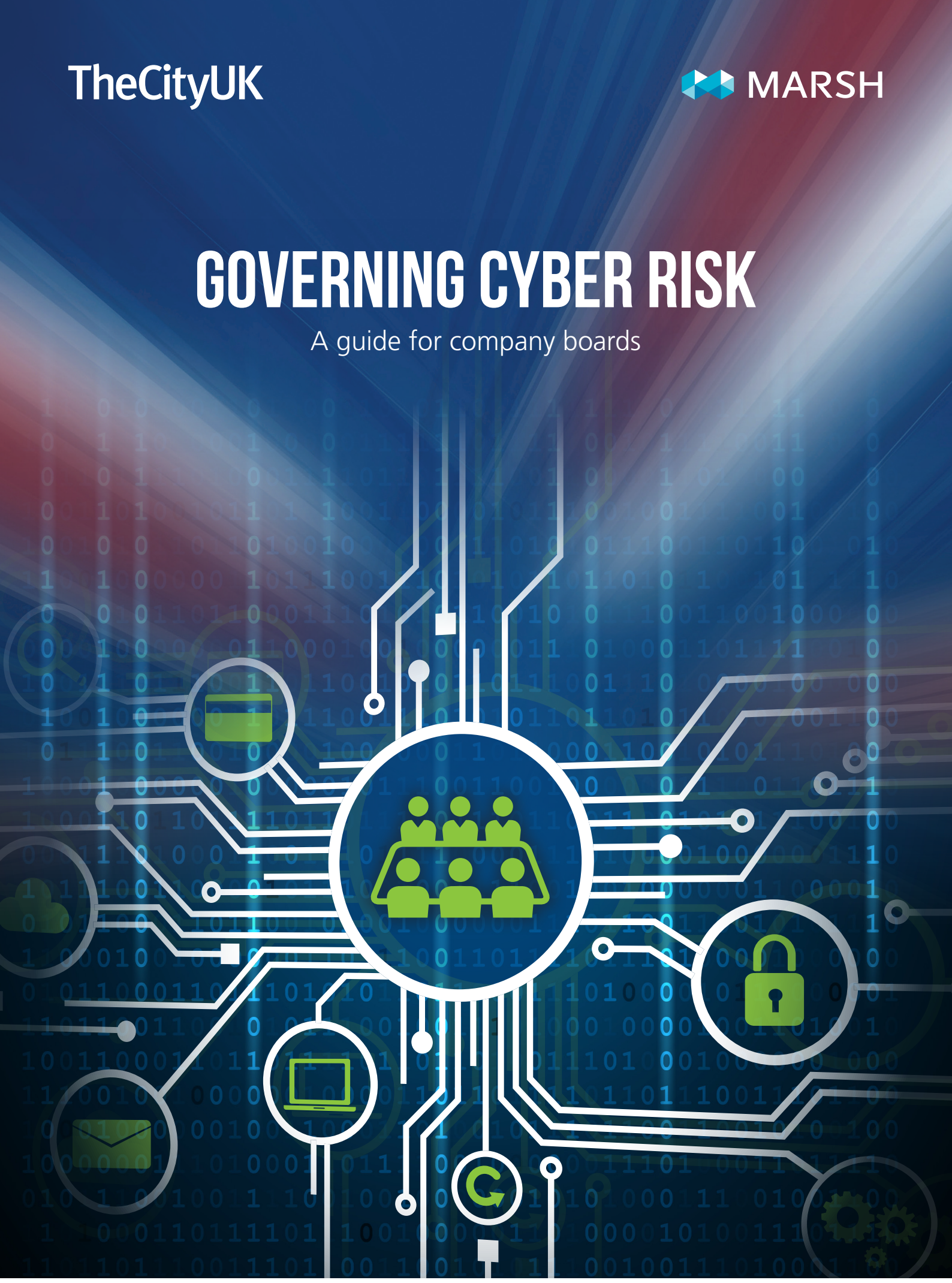
TheCityUK

MARSH

GOVERNING CYBER RISK

A guide for company boards



April 2018

@thecityuk www.thecityuk.com

About TheCityUK

TheCityUK is the industry-led body representing UK-based financial and related professional services. In the UK, across Europe and globally, we promote policies that drive competitiveness, support job creation and ensure long-term economic growth. The industry contributes nearly 11% of the UK's total economic output and employs 2.3m people, with two thirds of these jobs outside London. It is the largest tax payer, the biggest exporting industry and generates a trade surplus greater than all other net exporting industries combined.

About Marsh

A global leader in insurance broking and innovative risk management solutions, Marsh's 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

CONTENTS

FOREWORD FROM THECITYUK

Digital technology has radically changed people's lives and has brought untold benefits. Unfortunately, it has also brought with it cybercrime. Not only are criminals after our information, they are after our money, and can and will steal it where and whenever they choose, whether we are awake or asleep.

Criminals are harnessing this new digital reality, in which they can reach out across the globe, anonymously, and virtually risk-free. They are smart, highly innovative and persistent. The rewards are huge – it is the black market on steroids.

It is, though, a relatively new threat. It has taken little over a decade for cyber security to go from a niche issue to become a tier-one national security problem in every major state in the world, as well as for every individual and company.

Make no bones about it, cybercrime is a clear and present danger, not only to our current way of life, but also to society as a whole.

Our traditional defences are no longer adequate to protect ourselves as shared industry systems, companies or individuals. This is war, and needs wartime, not peacetime, urgency and defences.

So, managing this threat requires us all, and particularly boards of directors, to develop this sense of urgency and raise our game to protect ourselves, our companies and society.

This report, 'Governing cyber risk – a guide for company boards', commissioned by TheCityUK, in conjunction with Marsh, is intended to inform boards as to how to advance their governance of cyber risk and to provide practical guidance on what boards can do to ensure the security of their customers, their people and their companies.

I would like to thank everyone who has contributed to the development of this report, in particular Mark Weil, CEO, Marsh UK & Ireland and Chairman of TheCityUK Cyber Advisory Group, the members of that group, and the team at Marsh.
It is an important contribution to this vital debate.

John McFarlane
Chairman, TheCityUK

FOREWORD FROM MARSH

When it comes to cyber security, boards have a difficult job to do. On the one hand they need to ensure their companies are at the forefront of digital transformation so as not to be left behind; on the other hand they need to make sure that their companies are resilient to the cyber attacks which digital transformation will amplify.

There has been a lot of commentary on the technical aspects of cyber security, but less has been said about how boards can ensure that the right things are being done and in the right way. We aim in this report to provide board members with a guide to the governance of cyber risk and have deliberately avoided the jargon that surrounds the threat. Instead, we try to extract practical insights for boards on how they can best govern the risk.

Through our benchmarking, we have found big differences in boards' approach to cyber risk, but ones that are relatively easy to close given they are more a matter of attitude than expenditure. We want all boards to be confident that if a breach occurs, actions have been taken to minimise harm to their customers and to their company.

Mark Weil

CEO, Marsh UK & Ireland and Chairman, TheCityUK Cyber Advisory Group

SUMMARY

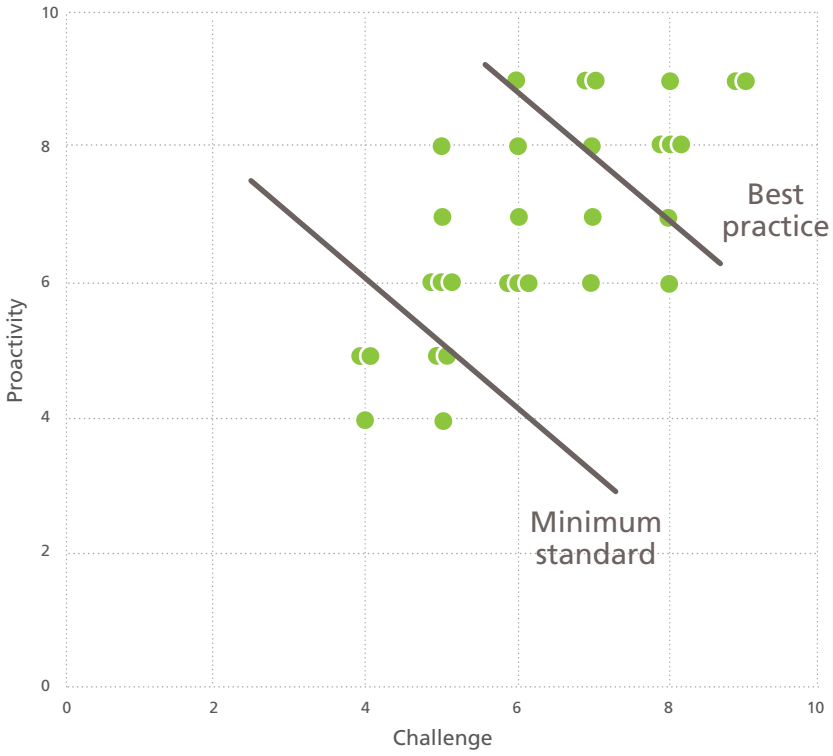
Benchmarking results

The research for this report was undertaken by engaging with 30 companies from across the financial and related professional services industry. All of these companies have management teams working on cyber security. However, at board level we found marked differences in the way they are governing that effort. The most engaged boards are proactive in taking ownership of the risk and ensuring that efforts are being made to manage exposure and prepare for a breach. They also challenge management by providing an independent view of what is being done, insisting on external validation and actionable, forward-looking reporting.

Figure 1 plots the results of the 30 boards' proactivity and challenge, based on six underlying elements of board benchmarking.

Figure 1: Framing benchmark responses as board proactivity and challenge

Source: TheCityUK and Marsh



The board's proactivity has been assessed on the basis of:

1. clarity of strategy

2. extent of board ownership

3. insight into financial resilience

The board's level of challenge has been assessed on the basis of:

4. executive accountability

5. independent assurance

6. board reporting

Figure 1 identifies a minimum standard to which we think a board should operate. Our research found that some of those interviewed fall below this standard, while several operate well above it. Cyber is a risk where herd immunity applies, particularly for companies trading closely together as members of the financial community. We therefore encourage companies to act to at least a minimum standard of proactivity and challenge, noting that we expect regulators will reach a similar conclusion.

For example, the Financial Conduct Authority (FCA) has said that they expect companies of all sizes to have a 'security culture' embedded in the organisation, which allows the business to protect its information assets, detect breaches and respond to and recover from incidents.[1] The Bank of England has also made clear in its public statements that the operational resilience of the financial system is of critical importance.[2]

This need not be onerous – it is mainly about approach and focus rather than expenditure and scale. Even a modest increase in the board's attention will lift the engagement of management on cyber risk.

At a more detailed level Figure 2 below summarises the three levels of maturity identified for each of the individual six elements we benchmarked against. It also displays the proportion of companies achieving each level for a given element.

Figure 2: Summary of the three levels of maturity for each element of cyber governance

Source: TheCityUK and Marsh

Element	Level 1	Level 2	Level 3	Proportion of companies achieving each level
Strategy	Prevention	Prevention and preparedness	Part of enterprise risk management	
Board ownership	Reactive	Proactive	Direction setting	
Financial resilience	Qualitative appreciation	Exposures quantified	Crisis finance plan in place	
Executive accountability	Standards set by security function	Chief Risk Officer oversight and challenge	Fits three lines of defence with board oversight	
Assurance	Self-evaluation by security function	External assessment and testing	Independent assurance across all aspects	
Reporting	Ad hoc, technical	Regular reporting on current state	Forward-looking aligned to risk reduction targets	

Key: Level 1 **Level 2** **Level 3**

[1] FCA , 'Cyber resilience', (July 2017), available at https://www.fca.org.uk/firms/cyber-resilience and FCA, 'Our approach to cyber security in financial services firms', (November 2016), available at https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms

[2] Bank of England Speech 'The Bank of England's approach to operational resilience' (13 June 2017), available at http://www.bankofengland.co.uk/publications/Documents/speeches/2017/speech979.pdf

Most companies interviewed are at Level 2 for most of the elements of board governance of cyber risk. While some are at Level 3, a number are at Level 1. In terms of differences by sector, the larger, balance sheet businesses (banks and insurers) tend towards Level 3, possibly reflecting their more mature infrastructure for managing risk and the significant amount of work from their regulators to encourage action.

Characteristics of boards at Level 1 and Level 3

The summary below helps to illustrate the differences in cyber risk governance between companies operating at a maturity Level of 1 and 3.

Characteristics of boards operating at Level 1:

- Minimal cyber strategy beyond not wanting to be breached.
- Ownership of risk is left to the security experts.
- Exhibit a limited appreciation of the threat.
- Cyber issues only discussed internally when they reach the newspaper headlines.
- Undertake little in the way of external assurance.
- Limited useful management information on which to base business decisions.

Characteristics of boards operating at Level 3:

- Clear strategy for cyber which permeates all major commercial decisions including its role in the customer proposition and a set direction for management on cyber risk. This includes quantifying exposure and the development of detailed plans for a possible breach.
- Responsibility for cyber security is based on the three lines of defence commonly used in risk management and defined in the methodology (found on page 21 of this report). These boards actively source and utilise a range of external validations and discuss cyber regularly against management information that is both forward-looking and actionable.

Of these aspects, we take the quality of management information being provided as the acid test of a board's ability to govern effectively. While there is no single definition of what constitutes the right information to see, we found examples where companies relied on retrospective updates on public breaches which provided large volumes of attack information with little synthesis or insight.

This could result in a board being exposed to the accusation that it was informed but failed to act. Those with the most convincing grasp on cyber risk governance are regularly seeing forward-looking information including progress against a defined improvement plan, security performance indicators and the status of validation exercises and breach response plans.

Cross-sector issues

The work also points to two areas in particular, education and infrastructure, where boards would benefit from cross-sectoral action.

Education

There is a gap in board information-sharing with respect to cyber risk governance. No matter how clear reporting becomes, boards will face complex, technical choices such as whether to rely on cloud providers or which accreditation path to follow. We see a role for cross-sector bodies such as TheCityUK to work with government departments, including the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre, to provide a forum for board-level education and information-sharing on cyber risk.

Infrastructure

Boards appreciate that their exposure to cyber risk can arise as much from vulnerabilities within their supply chains as from within their own IT. The outstanding issue of most concern to companies interviewed related to shared vulnerability to supply chain risk. Companies are particularly concerned about their collective dependence on a small number of infrastructure providers underpinning the UK's financial system architecture. Boards told us that they need a better way to work together to ensure that these risks are properly mapped and managed.

We recognise that most of these providers have their own governance and regulatory accountability. However, their importance is such that we believe the industry should explore a collective approach to assessing their cyber governance – as a public good for all users – rather than for each institution to be left to do so independently. This should include a focus on companies or platforms that have become sources of concentration risk for the industry.

Recommendations

In conclusion, we see good progress being made with cyber risk management, but there are some basic opportunities for boards to improve their governance of the risk to make sure that the right things are being done in the right way. We also see opportunities for companies to work collectively to improve the support they get with cyber risk governance as a public good for the industry as a whole.

We see a future role for bodies across the industry, including TheCityUK, in identifying and working with financial infrastructure providers – particularly those where high levels of concentration risk exist – to explore the possible development of a shared service assessment mechanism of cyber risk governance. This could include the development of an evaluation process that would feed into individual companies' governance as well as working with regulators to ensure that they provide appropriate scrutiny and support.

Recommendations

1. Boards should benchmark their own governance of cyber risk using the grid identified in Figure 2 to establish what actions they can take to move to Level 3.

2. Boards should confirm that they can answer positively to seven fundamental questions on cyber risk governance:

I. Have relevant statutory and regulatory requirements like the general data protection regulation (GDPR) been met?

II. Have cyber exposures been quantified and has financial resilience been tested?

III. Is an improvement plan in place to bring exposures within agreed risk appetite?

IV. Do regular board discussions take place on concise, clear, actionable management information (MI)?

V. Are breach plans in place which have been recently dry-run exercised, including at board-level?

VI. Are the roles of key people clear and aligned to the three lines of defence? See methodology.

VII. Is there independent validation and assurance, whether via testing, certification or insurance?

3. TheCityUK will seek to work with government departments, including the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre to develop a forum for education and information-sharing for board members on cyber risk governance.

4. TheCityUK will also seek to work with industry, regulators and government to identify sources of industry concentration risk and how these can be best managed.

INTRODUCTION

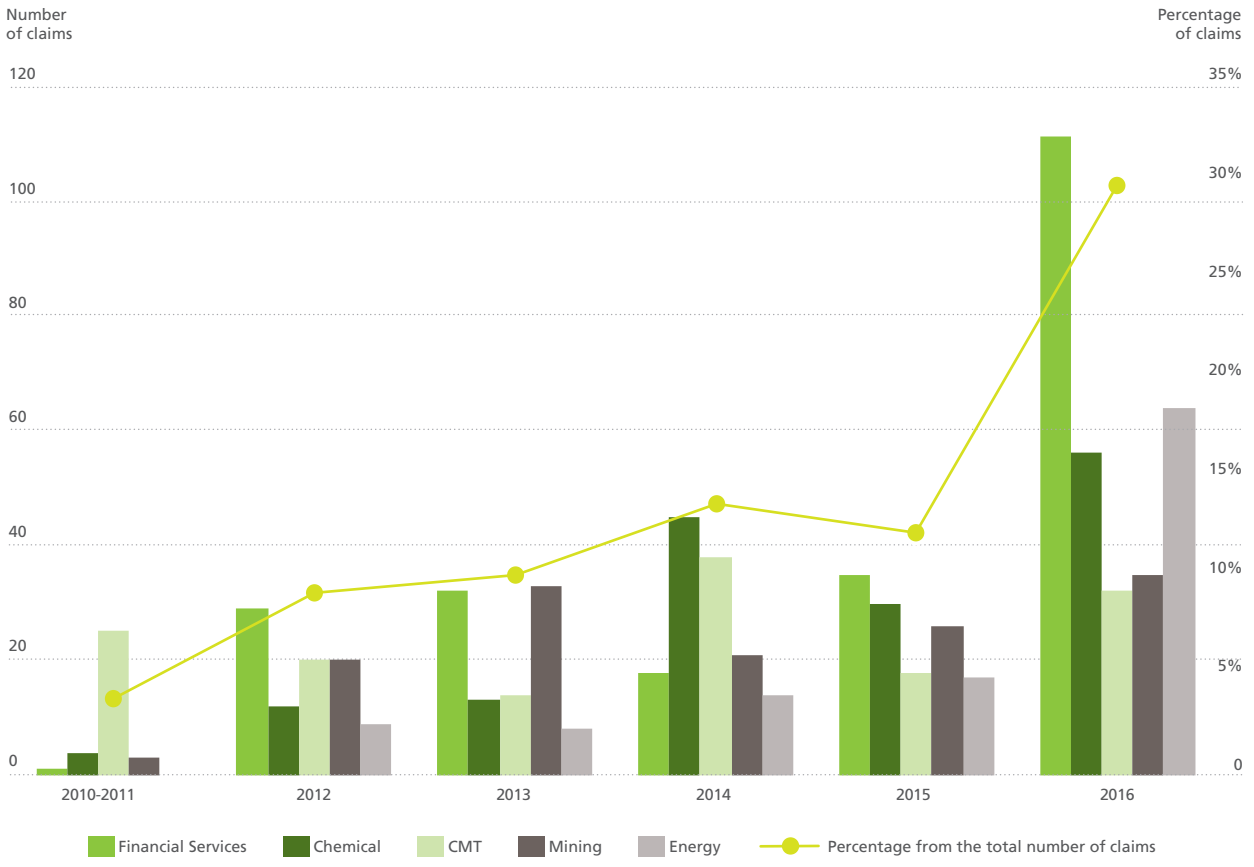
Boards have an unenviable task. They are the ultimate governors of risk, sitting between their management team and stakeholders including shareholders, supervisors and government and law enforcement agencies.

The pressure on boards to fulfil their risk governance role has increased. The UK Corporate Code sets out the requirement that "the board is responsible for determining the nature and extent of the principle risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems".[3]

There are a range of other requirements (see box on page 11), which expose directors and officers to increased liability, where they can be found personally accountable for their own and their organisations' actions across offences. These can include bribery, corruption, fraud, environmental law, health & safety, money laundering and misconduct. Penalties for breach can include disqualification, personal fines or even imprisonment. One consequence for the board, as evidenced in Figure 3 is a spike in claims under Directors & Officers insurance policies in the last year, led by the financial sector.

Figure 3: UK Directors and Officers insurance claims handled by Marsh

Source: Marsh



[3] Financial Reporting Council, 'The UK Corporate Governance Code' (April 2016) available at https://www.frc.org.uk/getattachment/ca7e94c4-b9a9-49e2-a824-ad76a322873c/UK-Corporate-Governance-Code-April-2016.pdf

UK directors fiduciary and regulatory responsibilities

Today's business environment is more complex than ever and company executives are facing an unprecedented amount of scrutiny into their actions. Areas of risk include:

- **Financial Reporting Council Corporate Governance Code:** the Code places the onus firmly on the board of directors of listed and non-listed companies to set the correct tone for their organisation and to take on greater personal accountability in the way they think about, manage and report on their principal risks and culture.
- **Financial Conduct Authority and Prudential Regulatory Authority's Senior Managers & Certification Regime (SM&CR):** the Senior Managers Regime currently requires senior individuals within the banking and insurance sectors (soon to be extended to all financial services companies) to demonstrate that they are taking responsibility for their actions.
- **GDPR:** greater controls are being imposed over the hosting and processing of personal data by organisations anywhere in the world. Directors can be held liable for their company's breach.
- **Bribery:** directors may be found liable along with their organisation if it is found that they consented to or participated in a bribery offence under the Bribery Act 2010.
- **Corporate Manslaughter and Health and Safety:** directors can be found liable under common law for the offence of corporate manslaughter and also under the Health and Safety at Work Act 1974 for a variety of workplace offences.
- **Modern Slavery Act 2015:** seeks to prevent modern slavery occurring in prescribed organisations and their supply chains. There may be repercussions for directors of those organisations that do not comply with the provisions of the Act.
- **Environmental Liability and Climate Change:** directors who don't properly consider climate-related risks could be liable for breaching their duty of due care and diligence.
- **Reporting:** disclosure requirements are increasing to support greater transparency, including those relating to the Gender Pay Gap, Prompt Payment and Tax Transparency. Directors can be found liable under the Fraud Act 2006 of dishonestly failing to disclose information which they are under a legal duty to disclose or under the Theft Act 1968 for making a false statement as to the affairs of a company with the intent of deceiving shareholders or creditors.
- **Companies Act and Common Law Duties:** directors are required, not only to promote the success of the company, but to take into account the longer term consequences of decisions.

To this plethora of risks, we must now add the cyber threat. Cyber gives boards the dual problem of driving management teams to avoid being left behind in the race to digitise while dealing with the increased exposure to cyber attack that technological dependency brings.

There has been a strong management response to this threat in the last three years through a combination of board, regulator, customer or vendor pressure and awareness. There has also been a dramatic increase in activity, for example, reflected in numerous surveys of corporate engagement on cyber risk.

Most large companies now have cyber improvement programmes in place. These typically include investment in technical and security controls, external testing and accreditation, cyber incident response plans and information-sharing across peers.

A great deal of support for companies has been made available through the work that governments, industry bodies and other organisations have done, including the development of standards and best practice guidance. These help to strengthen technical and security operations, providing frameworks and checklists that can be used to drive management action and to benchmark performance against peers.

However, it is boards that sit at the top of the pyramid of accountability. In contrast to managing the technical and operational aspects of cyber risk, there is limited opportunity for boards to compare different approaches being taken and no equivalent set of standards for a board to benchmark itself against. Without such inputs, boards may find themselves over-reliant on management experts, and uncertain about how to provide effective challenge.

Ultimately, it is for boards to ensure that the right actions are being taken, and that the people undertaking them are meeting the levels of performance required. In some of the more public breaches, with the benefit of hindsight, relatively basic challenges set by the board might have led to better decisions being taken on security measures and crisis response.

This report aims to help boards enhance their governance of cyber risk. It does so by looking purely at board actions to strengthen cyber risk governance, rather than at the technical and operational aspects of cyber risk. We take it as a given that companies have appreciated the magnitude of the cyber threat and are acting on it.

We therefore don't focus on aspects of the cyber threat dealt with elsewhere, for example the nature of the risk, the diversity of malefactors and routes to harm, or the potential impact of the risk on finances and reputation. However, we do note the growing dependence of companies on external infrastructure and suppliers such as cloud providers. That means that governance considerations need to extend beyond the perimeter of the company to include supply chain risk, in particular those suppliers who are critical to the functioning of the financial system.

Figure 4: Cyber risk management pyramid of accountability

Source: Marsh

BENCHMARKING CYBER RISK GOVERNANCE

We identified six elements against which to benchmark cyber risk governance (and which can broadly apply to governance of any risk).

1. **Strategy:** how well does the board understand the company's priorities and strategic approach to cyber risk and to what extent is cyber risk being factored into broader board-level decision making?
2. **Board ownership:** to what extent does the board drive the strategy and how well is it integrated into board-level risk management processes?
3. **Financial resilience:** are cyber risks quantified and built into a stress-tested crisis recovery plan?
4. **Executive accountability:** how are executive responsibilities for cyber risk management structured and how are individuals held to account?
5. **Assurance:** where does the board get validation that cyber risk has been properly assessed and that the management response is robust?
6. **Reporting:** how is the company's cyber risk position and progress reported to the board?

Against each element we then defined three levels of maturity based on the findings of the 30 interviews. This section discusses the levels of maturity in more detail, as well as illustrating the scoring and providing a sample question set to help boards reach a Level 3 maturity.

Strategy

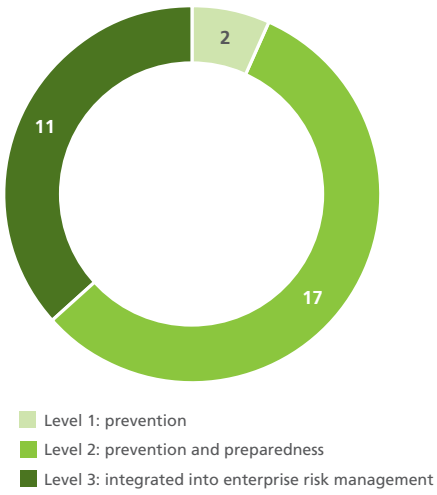
Is there a defined approach to the risk?

Levels of maturity

1. **Prevention:** the board is aware of cyber risk, understands the importance of investing in preventative controls, but does not go any further in terms of specificity or directing activity.
2. **Prevention and preparedness:** the board has recognised the risk of a breach occurring and has directed a portion of its scrutiny to making sure that preparations have been made to cope.
3. **Integrated into enterprise risk management (ERM):** the board has a clear understanding of how cyber risk impacts on the business and has set a level of cyber risk appetite. Cyber risk is factored into a broader set of decisions including strategy-setting, investments, acquisitions, and as a component of the customer proposition.

Figure 5: Strategy – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



All companies interviewed identified cyber as a top tier risk, reflecting the general progress that has been made in recent years on raising the profile of cyber risk at board level. Companies also recognised that cyber risk could not be eliminated entirely, and most had crisis response plans in place – many had conducted dry-run exercises with board members participating.

Many companies nonetheless tended to treat cyber risk in isolation from other elements of their ERM framework, not always recognising the interplay between cyber risk and other aspects of board-level decision making.

Critically, leading companies treated high standards for IT and security operations as a necessary but not sufficient goal. They have recognised that cyber risk can stem from many different sources, such as employees and suppliers, and so has many facets to it (such as recruitment policies, employee engagement and training). They have accordingly integrated cyber into the broader risk management arrangements of the business.

A number of companies had looked beyond cyber as a source of risk, and were starting to consider how they might be able to leverage their investment in cyber to add value to their customers – either as a market differentiator, or as the basis for enhanced security-based products and services.

Sample questions set to help boards reach Level 3 of maturity:

1. How well does the board understand the company's priorities and strategic approach to cyber risk?
2. What improvement activities are in place to bring cyber risk within tolerance?
3. To what extent is cyber risk being factored into broader board-level decision making? This might include aspects such as strategy-setting, investments, acquisitions, and as a component of the customer proposition.

Board ownership

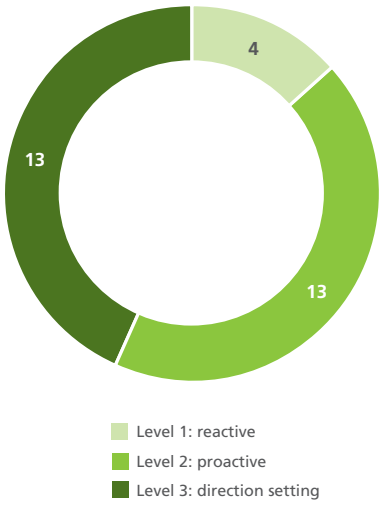
Is the board engaged in setting the direction and monitoring progress and performance?

Levels of maturity

1. **Reactive:** the board responds to cyber issues and plans as presented by management, but without taking ownership or having the expertise to lead.
2. **Proactive:** the board educates itself on cyber matters to the point where it can help to prioritise action and be a significant contributor to the debate.
3. **Direction setting:** the board has formed a position on cyber risk and the stance it wishes to take and directs management towards that position.

Figure 6: Board ownership – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



All companies interviewed include cyber risk as a formal board agenda item. In a small number of cases, the board members lack the expertise to engage and challenge – instead being recipients of occasional briefings and investment plans rising up from the business.

Most boards have taken proactive steps to ensure that they were informed about various aspects of cyber risk, the threat environment, and how this relates to their particular company. Leading boards have been actively involved in setting overall priorities for the company's cyber improvement programme and regularly hold the executive to account on progress against that plan.

One element of board engagement is the attention paid to their individual duty. Leaders are briefed on their duty and exposure, including the support in place such as how Directors & Officers insurance would respond to cyber-related matters. More broadly, we noted a range of methods board members were using to inform themselves on cyber risk:

- Regular briefings on duties created by new regulation and legislation such as SM&CR and GDPR.
- Board and executive committee joint exercises.
- Visits to best practice peers and leaders on cyber security.
- Security briefings on threat environment.
- Board-level exchanges of information on governance and reporting.

Sample questions set to help boards reach Level 3 of maturity:

1. How are the priorities for the company's cyber improvement activities being set? What role has the board played in this process?
2. What role would the board play in the event of a serious cyber incident?
3. How does cyber risk affect board members own fiduciary and regulatory responsibilities?

Financial resilience

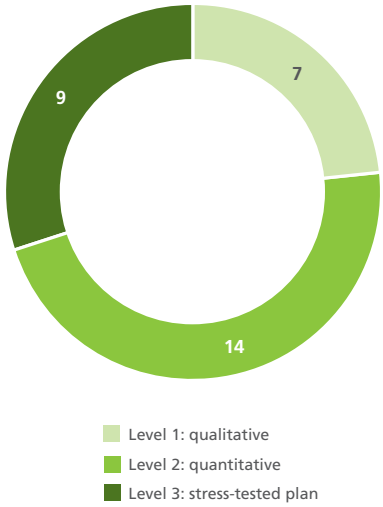
By financial resilience, we mean the extent to which the potential impacts of adverse cyber events on the business have been assessed in terms of the company's ability to absorb the cash and capital impacts they could face, as well as the broader crisis response.

Levels of maturity

1. **Qualitative appreciation:** the board has a broad appreciation of what might happen, typically informed by public cases of breaches to companies in the same sector but without specific scenarios identified or their impact quantified.
2. **Exposures quantified:** the board has seen quantification of the risk based on scenarios most relevant to their company. That quantification may be done using expert input, case studies and known parameters such as regulatory sanction to create stress-tests for cyber risk.
3. **Stress-tested crisis response plan:** the board has a fully stress-tested crisis finance plan and has considered the forms of risk finance available, such as insurance.

Figure 7: Financial resilience – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



Companies varied in terms of the extent to which they had sought to quantify their cyber risk exposures. Some argued that quantification is virtually impossible to do given the new and open-ended nature of the threat – while others highlighted the risk that quantification could lead to overly conservative assessments that could in turn lead to complacency. Most nonetheless agreed that some quantification of specific threat scenarios helped them to undertake crisis planning and to prioritise mitigating actions.

In some cases, full quantification exercises had been completed, either as part of broader Basel/Solvency II related activity, or as part of more general crisis management planning such as Recovery and Resolution Plans. In looking at financial resilience, leaders had a good handle on their ability to absorb impacts, giving consideration to the restricted access they might have under stress to their revolving credit facilities and other lines of credit. Equally, they had looked at their insurance programmes as a supplementary source of finance, noting that some cover may come from traditional policies before invoking the need to purchase cyber insurance specifically.

Sample questions set to help boards reach Level 3 of maturity:

1. What would a worst case cyber incident cost the company and would it be able to trade through any reputational impact?
2. How would the company finance such a crisis, noting the restricted access to credit under stress?
3. What protection does the company's insurance programme provide as a part of the wider crisis finance plan?

Executive accountability

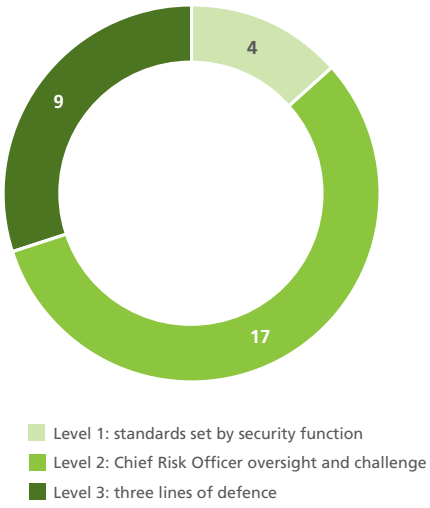
By executive accountability, we mean the way in which roles and responsibilities within the executive are structured and how individuals are held to account.

Levels of maturity

1. The security function operating in isolation.
2. Formal oversight and challenge provided by the Chief Risk Officer (CRO).
3. Cyber fully integrated into the three lines of defence model (see methodology), with board oversight.

Figure 8: Executive accountability – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



The Chief Information Security Officer (CISO) plays a central role in cyber risk management at all the companies interviewed. However, the CISO's line of accountability varied, including reporting to the Chief Information Officer, CRO and Chief Operating Officer. Some had created hybrid arrangements, with the CISO reporting to multiple chief officers.

While there is no single right way of structuring this, in the leading companies roles are made to fit into the three lines of defence, (see methodology) which commonly meant that the CISO sits in the first line of defence and is overseen and challenged by the CRO in the second line. This avoids the problem we heard several times of CISOs being "line one and a half", which effectively means they mark their own work. It also has the advantage of avoiding defining cyber risk too narrowly, as just a matter of internal IT and security operations. The CRO will tend naturally to look at wider risks and dependencies created by cyber including vendors, employees and customers.

Sample questions set to help boards reach Level 3 of maturity:

1. Who is accountable for managing cyber risk?
2. Who is holding them to account, and how?
3. How is cyber risk integrated into the company's three lines of defence model?

Assurance

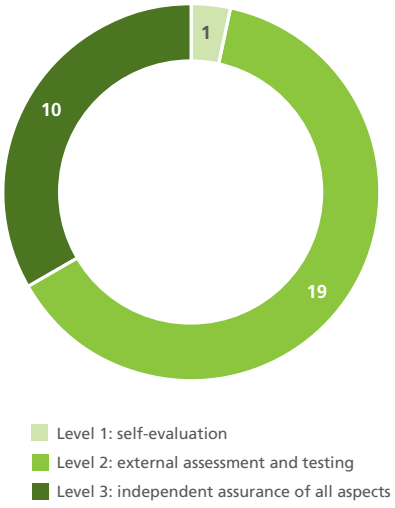
By assurance, we mean the extent to which the board has access to independent validation that the information that they are receiving, and the options that they are being given to decide upon are robust and reliable.

Levels of maturity

1. Self-evaluation by the security function.
2. External cyber assessment and testing.
3. Independent assurance of all aspects, IT and security, supply chain risk, business continuity and financial resilience.

Figure 9: Assurance – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



Most companies interviewed used one of the main regulatory or industry standards such as the National Institute of Standards and Technology (NIST) to assess their core cyber security functions. However, in most cases the scope of the assurance was restricted to internal IT and security issues (ignoring supply chain risk, financial resilience and crisis management) and in some cases is self-assessed by the security function itself.

All the companies interviewed had developed cyber incident response plans, and most had exercised them in dry runs. However, these plans varied in scope. Some were focused primarily on IT system recovery, while others engaged with the broader issues of financial stability, reputation management and customer care.

Most companies have sought external cyber security evaluation and testing. Again, however, this external evaluation rarely went beyond internal systems issues to consider the broader response plan.

Finally, some companies had purchased cyber insurance, in part for the financial benefit, but mainly for the validation that comes from an insurer betting their money against a company's likelihood of breach. To quote the chairman of a major bank, "if I can get more cover and for less than my competitors pay, I know my team are telling me the truth."

Sample questions set to help boards reach Level 3 of maturity:

1. How has the effectiveness of the company's cyber defences and crisis response plans been assessed?
2. How is the company exposed to cyber incidents in the supply chain, and how have these suppliers' own cyber security measures been assessed?
3. What access does the board have to independent advice on the decision making and performance of relevant accountable members of the executive?

Reporting

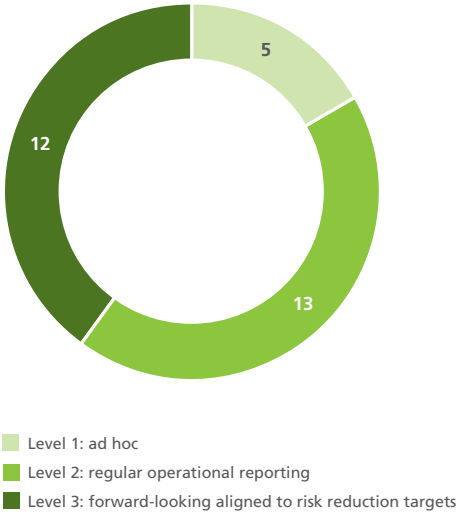
By reporting, we mean the quality of information being presented to the board and specifically the ability to check progress, confirm preparedness for a breach and validate choices.

Levels of maturity

1. Ad hoc, technical updates.
2. Regular reporting on the current performance of the cyber function.
3. Forward-looking reporting linked to risk reduction targets.

Figure 10: Reporting – number of interviewees at each level of maturity

Source: TheCityUK and Marsh



We found reporting to be a good acid test for the true state of governance. The question of what the board actually sees as a regular report leaves little place to hide and most of those we interviewed, when challenged, admitted to frustrations with the information being provided to them. A number of companies, however, had invested significant time and effort to developing their reporting frameworks, and some best practice approaches are beginning to emerge.

Figure 11: Principles of effective board reporting

Source: TheCityUK and Marsh

Reporting principle	Rationale
Concise	The volume of material should not compensate for quality. Excessive length transfers the burden of filtering and interpretation to the board. In the event of a breach or issue this could leave the board exposed to the accusation of having 'been told' but not then acting.
Clear	Reporting on cyber often contains high levels of jargon and technical terms. Those providing reports need to make sure that they are clear in what they say and don't hide behind obscure or ambiguous language.
Actionable	Reporting needs to provide a basis for decisions. There is a useful distinction between 'run' and 'improve' reporting, with the former focusing on current performance of the security function and the latter on what is being done to raise standards and deliver improvement programmes. In both cases, the information provided should allow the board to act.

Many of the board members interviewed said they would welcome a best practice template for cyber risk reporting. While it is hard to define a single template, we highlight below some of the information that we think a standing – and ideally at least biannual – report on cyber risk should cover:

- Status of compliance with statutory and regulatory requirements.
- Status of compliance with other relevant cyber security standards (NIST, 10 Steps etc.).
- Statement of gross and net exposures (strategic, financial, operational) and risk appetite and an improvement plan to bring exposures within agreed risk appetite.
- Performance of the security function (breaches, near misses, lessons learned from tests, updated breach plans in place following these tests).
- Supply chain compliance and performance.
- Progress on the improvement plan (and impact on exposure to cyber risk).
- Significant external events, implications for the business, and recommended actions arising.
- Assurance statements from accountable executives.

Sample questions set to help boards reach Level 3 of maturity:

1. Has the board set out a schedule of reporting – both to the main board as well as relevant committees – on cyber risk?
2. Does the scope of the reporting include the elements above?
3. Is the board taking clear and meaningful actions as a result of this reporting?

CONCLUSIONS

The 30 companies we interviewed have all made good progress with cyber risk management and most of the early strictures on the need to act on defence and preparedness for a breach have been followed. However, we saw a material difference in the proactivity and challenge being provided by boards as illustrated in Figure 1.

There is no single right way of structuring cyber risk management within an organisation. However, we can extract some practical steps and boards should confirm that they can answer positively to seven fundamental questions on cyber risk governance.

I. Have relevant statutory and regulatory requirements like the GDPR been met?

II. Have cyber exposures been quantified and has financial resilience been tested?

III. Is an improvement plan in place to bring exposures within agreed risk appetite?

IV. Do regular board discussions take place on concise, clear, actionable MI?

V. Are breach plans in place which have been recently dry-run exercised, including at board-level?

VI. Are the roles of key people clear and aligned to the three lines of defence? See methodology.

VII. Is there independent validation and assurance, whether via testing, certification or insurance?

Reporting in particular is a good indicator of the extent to which boards are getting a grip on cyber risk. Many companies have invested significant time and effort over the past few years in improving the quality of reporting, and some best practice principles are beginning to emerge as detailed in the section on reporting in the benchmarking chapter.

Improving cyber risk governance need not be expensive. The differences between the leaders and the laggards depends not so much on inputs such as technology or spend, but more on outputs and outcomes such as the allocation of responsibilities, monitoring and reporting. Given the contamination risk across companies doing business together, we expect that over time a high bar will be set across the industry, whether driven by boards, customer pressure or regulators.

An important first step will usually be improving the board's understanding of cyber risk. The educational activities we observed among the boards we interviewed include:

- Regular briefings on duties created by new regulation and legislation such as SM&CR and GDPR.
- Board and executive committee joint planning and breach response programmes visits to best practice peers and leaders on cyber security.
- Security briefings on threat environment.
- Board-level exchanges of information on governance and reporting.

Cyber education and information-sharing has to date been more technically focused and less relevant to the board. Given the importance of board governance, we therefore see an opportunity for cross-industry bodies to look at how boards can be informed on cyber matters.

Finally, we note the burden on boards to govern not just their own risk but that emanating from suppliers, many of whom are used across the industry and represent critical infrastructure. Given the difficulty and duplication in each company monitoring those providers we believe there is scope for a collective approach – both in assessing common providers and ensuring that they are being given due priority by authorities given their importance to the financial system.

AUTHORS AND METHODOLOGY

The taskforce for the publication of the report comprised the following members:

- Mark Weil, CEO, Marsh UK & Ireland (Chairman, TheCityUK Cyber Advisory Group)
- Marcus Scott, COO, TheCityUK
- Philip Jones, TheCityUK
- Charlie Netherton, Peter Johnson, Jamie Saunders, Marsh Ltd.

Contributors

- The core of the report is built on benchmarking interviews with 30 members of TheCityUK, between October 2017 and March 2018, as illustrated by the sector breakdown below.
- Interviewees were Chairmen, Non-Executive Directors, Chief Executive Officers and other senior accountable executives from a cross section of TheCityUK membership.
- TheCityUK Cyber Advisory Group (https://www.thecityuk.com/about-us/working-groups/cyber-advisory-group/).

Sector	Count of interviews
Financial institutions	12
Insurance companies	5
Professional services	5
Investment managers	4
Law firms	4

The research started by using expert and board member input to help define the critical elements of governance. This gave us six elements of cyber risk governance (and which can broadly apply to governance of any risk). We then used the interviews to refine and validate those elements and allocate a company-specific level of maturity to each element.

Interviews were undertaken using a structured discussion guide based around the six elements of benchmarking. We also added open-ended questions to identify contextual factors and explore wider issues such as government and regulatory activity on cyber risk.

Initial findings were discussed among the project team and TheCityUK Cyber Advisory Group to help refine the benchmarking dimensions and insights being drawn.

Finally, emerging conclusions from this work were presented to TheCityUK Advisory Council for discussion and input to this report.

Three lines of defence

The term 'three lines of defence'[4] is used a number of times in this report as short hand for the standard methodology used to manage risk. This is explained, clearly and usefully, by the Chartered Institute of Internal Auditors as follows:

1. The first line of defence – functions that own and manage risk.
2. The second line of defence – functions that oversee or specialise in risk management, compliance.
3. The third line of defence – functions that provide independent assurance, above all internal audit (and its attendant Board governance, such as the Board's Audit Committee).

[4] Further details can be found on the IIA website at https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/ and on the ISACA website at https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Three-Lines-of-Defence-Related-to-Risk-Governance.aspx

For further information about this report contact:

Marcus Scott, COO, TheCityUK
marcus.scott@thecityuk.com
+44 (0)20 3696 0133

Philip Jones, Head, Africa, Middle East & Legal Services, TheCityUK
philip.jones@thecityuk.com
+44 (0)20 3696 0126

TheCityUK

TheCityUK, Salisbury House, Finsbury Circus, London EC2M 5QQ
www.thecityuk.com