



Governance in focus

Cyber risk reporting in the UK

February 2017

Contents

Foreword by William Touche: Reporting on cyber risk	01
1. Do companies describe cyber risk clearly?	03
2. Do boards demonstrate ownership?	09
3. Are mitigating activities well explained?	11
4. Are cyber security breaches described?	15
5. Professional guidance	16
Further resources	18
Appendix: How to disclose cyber risk	20
Contacts	22
About the Deloitte Academy	23

Reporting on cyber risk



Foreword from William Touche

Dear Public Company Director,

This is a first picture of cyber reporting across UK plc. We hope you find our findings valuable. As you would expect, we found a varied picture, and you will find the results of our analysis stimulating. You will be aware that cyber crime is growing more rapidly than cyber security, and organisations have never been more at risk from cyber attacks. Recent high-profile attacks on companies in the retail, media and industrial sectors have highlighted the type of damage that can be done by hackers and cyber terrorists. This growing threat comes at a time when there is also increasing focus from investors and regulators on how organisations manage risk.

Company directors are informing themselves about the types of cyber threat their company faces, and the most important information assets and systems to monitor and protect. They are also much better prepared to respond to a successful attack – and know who would be the company's spokesperson in the case of a major data breach. It is not a question of whether there will be cyber attacks, it probably never was, but it is a question of when, by whom and with what degree of expertise your company will be attacked.

In October 2016, the UK Financial Reporting Council (FRC) wrote to audit committee chairs and finance directors, commenting that they “encourage companies to consider a broad range of factors when determining the principal risks and uncertainties facing the business, for example cyber security”. Some investors have gone so far as to call for “a compulsory rigorous external cyber audit”.¹ The value destruction capability of a cyber attack is very high and therefore risks and mitigating activities should be sufficiently highlighted to investors to enable them to make informed decisions.

In the USA, the AICPA is developing new guidance around company reporting on cyber risk. It has proposed not only a description of the entity's cyber risk management programme but also an assessment of the effectiveness of the controls that are part of the programme. SEC guidance on cyber risk disclosure also exists and is a good and thoughtful framework which we have taken into account in forming our survey questions. Such regulatory developments are rarely isolated and we encourage UK listed companies to be on the front foot when it comes to high quality reporting in this area.

This is the very first survey of cyber reporting practices covering the full FTSE 100 and it should help you identify examples of good practice and will offer insight to all listed companies about how to keep the users of annual reports informed.² We have included a helpful summary to enable you to identify potentially worthwhile additions to your existing reporting in the appendix.

Our analysis examined whether the FTSE 100 are identifying cyber as a principal risk, how they are categorising and describing the risk and its impact. We have looked particularly at cyber crime, and whether they have reported an increase in the level of cyber risk since the prior year.

We have considered how clearly companies are describing the ownership of cyber risk and whether the board is leading the way and demonstrating that they provide appropriate challenge to management. In our view, the time is coming when boards will want greater expertise and experience around the table for specialist areas such as technology.

¹ FT Adviser article, December 2, 2015

² The survey covers the annual report published most recently as at 30 September 2016 for all FTSE 100 companies

“...We know that with new opportunities come new vulnerabilities. So alongside the ability to transact, process and store data on an unprecedented scale so comes the risk of being compromised on an unprecedented scale”

Ciaran Martin, CEO of National Cyber Security Centre in UK

Because of the importance of cyber risk, its constant evolution and the scale of potential impact, we would expect it to be a focus area on every board's agenda. The findings show that boards are not taking sufficient credit for the activity they undertake regarding cyber risk by describing their activities in their report for the year. As this is an area of interest to investors, we would encourage boards to ensure cyber risk does not “slip through the net” when finalising reporting.

So, what can we conclude from a review of FTSE 100 annual report disclosures?

- Every sector, although not every company, identifies cyber as a principal risk – think carefully if you have not done so.
- The value destruction capability of cyber risk is very high, ranging from remediation demands to huge reputational damage. Detailed disclosure is therefore worthwhile to highlight the risks to shareholders and lets them know you are taking it seriously.
- The better disclosures are company specific, year specific and provide sufficient detail to give meaningful information to investors and other stakeholders.
- Boards and board committees are increasingly educating themselves about the cyber threat and challenging management on how they are dealing with the risk.
- Companies should take credit for what they are doing, including describing who has executive responsibility, board level responsibilities, the policy framework, internal controls, and disaster recovery plans.
- Boards should think about what could be missing from their disclosures. We have provided some useful pointers in the appendix.
- Finally, if your disclosure does not look strong enough after taking credit for what the company is doing already, it is time to ask whether you are actually doing enough to manage cyber risk.

Whilst the digitally connected world of course presents threats, it also presents huge opportunities for those nimble enough to embrace them. The opportunity is not just about new business models, but also about the increased engagement with customers and suppliers, enabling better information exchange, increased efficiency and value accretion.

Do get in touch with your Deloitte partner, the cyber risk and crisis management specialists named in the contact list or my Deloitte governance team if you would like to discuss any areas in more detail. And don't forget you can join us at the Deloitte Academy where we host live updates to air current issues and enable you to swap notes with your peers.

Yours faithfully,



William Touche
Vice-Chairman
Leader of Deloitte UK Centre for Corporate Governance

1. Do companies describe cyber risk clearly?

In this section, we look at whether cyber has been identified as a principal risk in the strategic report. If so, we ask how those risks have been categorised – for instance as strategic or as operational risks – and whether companies have disclosed a change in the likelihood of the risk since their previous annual report.

87% of FTSE 100 companies disclosed cyber as a principal risk

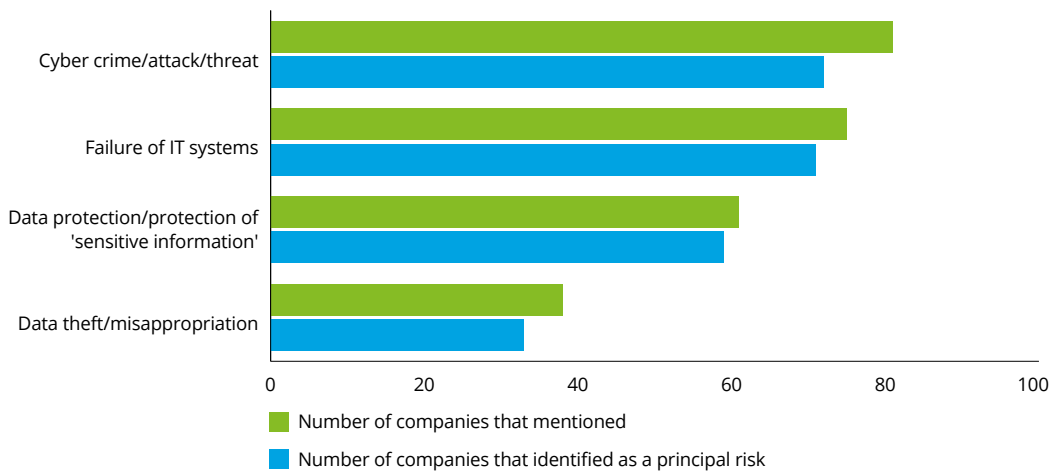
We also look at how specific companies have been around their exposure to different types of cyber crime and how companies described the potential impact of cyber risk on their operations.

1.1 Did companies recognise cyber risk as a principal risk?

We started by seeing whether cyber risk was identified in the annual report of each FTSE 100 company. Only five companies did not mention cyber risk; four of these were in the mining industry and one in the construction industry.

We identified four key elements reported in relation to cyber risk: cyber crime, IT systems failure (not necessarily related to cyber crime), data protection (the risk of data loss) and data theft or misappropriation. When defining their principal risks some companies focused on one (or two) of these key elements, and although some are more relevant to certain companies, in our opinion the better disclosures we saw incorporated discussion of all key cyber risk elements.

Figure 1. Types of cyber risk identified in FTSE 100 annual reports



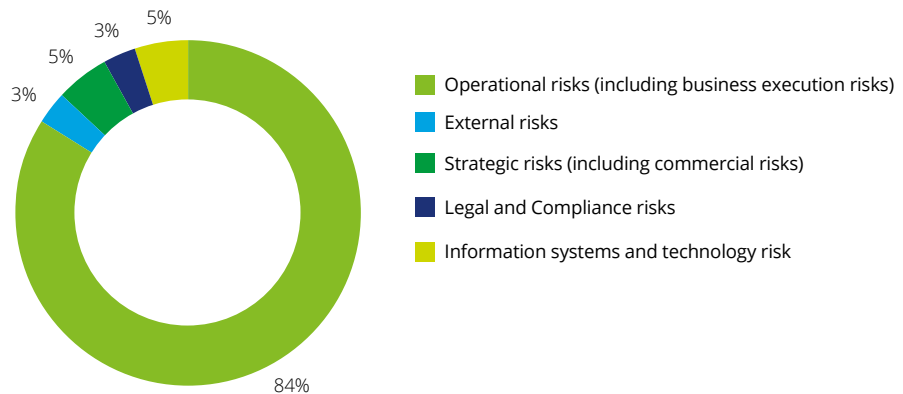
87% of the FTSE 100 clearly pulled out one or more elements of cyber risk as a principal risk in their disclosures. IT systems failure was identified in the principal risks disclosure by 71% of the FTSE 100 and cyber crime or cyber attack was identified by a slightly higher 72%.

Data protection risk – the risk around sensitive information, in particular compliance with data protection regulations – was identified by 59% while data theft or misappropriation of data, including intellectual property (IP) was specifically identified as a risk in only 33% of annual reports – although of course some companies will see this as falling under a broader risk of cyber crime.

For one third of the FTSE 100 to call data theft out as a principal risk indicates just how reliant we all are on technology, and how this increases our vulnerability.

64% of companies recognise that cyber risk is increasing year on year

Figure 2. Cyber risks as categorised in FTSE 100 annual reports (%)
Presentation of cyber risk in principal risk section by category



Most of the companies that categorised their principal risks recognised cyber risk as part of operational risk.

Some reports grouped cyber risks together with the risk of catastrophic events, due to their potential major impact.

1.2 Did companies disclose a change in the likelihood of the risk since the prior year?

A clear majority (56 companies or 64%) that included cyber risk as a principal risk also mentioned that the risk has increased compared to the previous year; 30 companies (34%) did not mention any change in the risk and one company (in the financial services sector) reported that the risk has decreased for them, although without further explanation. This last disclosure was unexpected as our experience is that financial services companies face an ever-increasing level of threat as one of the key industries targeted by cyber crime.

The better disclosures we saw acknowledged and explained an increase in cyber risk irrespective of the number and quality of mitigating actions undertaken.

Barclays plc 2015 annual report (p.122) clearly explains the rationale behind the increase in the risk in their disclosure:

i) Cyber attacks (emerging risk)
The risk posed by cyber attacks continues to grow. The proliferation of online marketplaces trading criminal services and stolen data has reduced barriers of entry for criminals to perpetrate cyber attacks, while at the same time increasing motivation.

Attacker capabilities continue to evolve as demonstrated by a marked increase in denial of service attacks, and increased sophistication of targeted fraud attacks by organised criminal networks. We face a growing threat to our information (whether it is held by us or in our supply chain), to the integrity of our financial transactions, and to the availability of our services. All of these necessitate a broad intelligence and response capability.

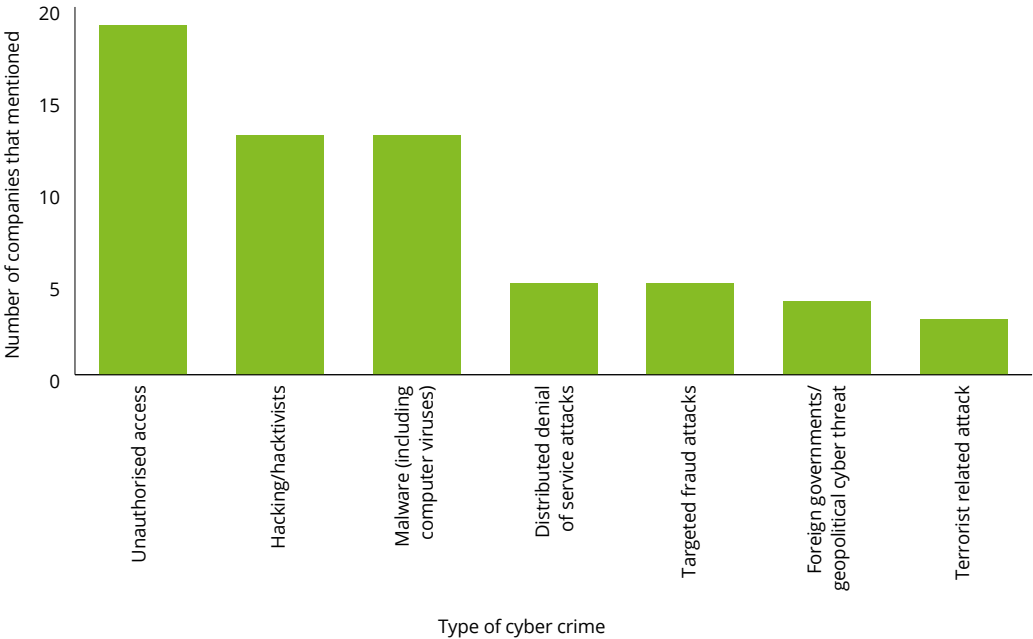
Given the level of increasing global sophistication and scope of potential cyber attacks, future attacks may lead to significant breaches of security which jeopardise the sensitive information and financial transactions of the Group, its clients, counterparties, or customers, or cause disruption to systems performing critical functions. Failure to adequately manage cyber threats and to continually review and update processes in response to new threats could result in increased fraud losses, inability to perform critical economic functions, customer detriment, regulatory censure and penalty, legal liability and reputational damage.

1.3 Were companies specific about the types of cyber crime they face?

Companies that are more specific about the nature of the cyber crime they have experienced or believe they are exposed to are more likely to be more specific about the management or mitigation they seek to apply (see section 3) – this of course encourages better disclosure overall.

The more specific the description of the risk, the better the disclosure of risk mitigation activities

Figure 3. Types of cyber crime FTSE 100 companies disclose they face



The most common threat mentioned was unauthorised access to systems (19%), a threat broadly faced by all companies with digital assets.

Other threats included reference to hacking and/or hacktivists (13%), malware (including computer viruses) (13%), denial of service attacks (5%), targeted fraud (5%), acts of terrorism (3%) and a few even mentioned foreign governments/geopolitical threats (4%). It was more common to see specifics about the nature of threats faced from companies in the financial services sector.

Disclosing this level of detail about the nature of the cyber risk a company is exposed to can help demonstrate to investors and wider stakeholder groups that the directors and management clearly understand the threats facing their organisation and management is therefore better able to develop appropriate mitigation strategies.

And the impacts?

- Disruption to operations
- Damage to reputation
- Loss of data
- Financial loss
- Regulatory fines

1.4 How did companies describe the impact of cyber risk?

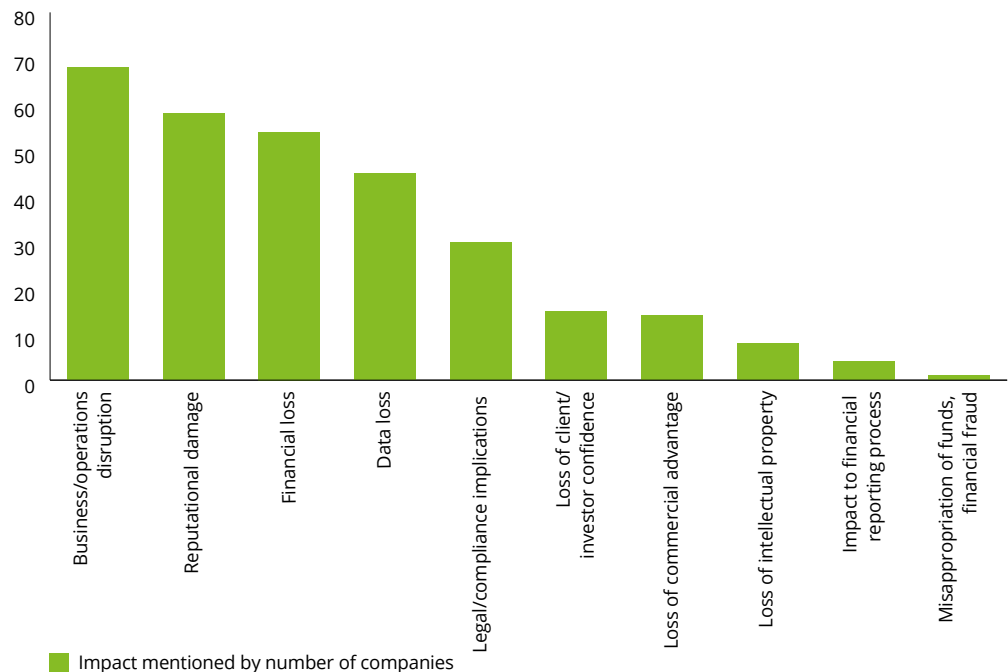
The most common impact, mentioned by 68% of the FTSE 100, was the potential disruption of business/operations, 58% mentioned reputational damage, and 45% mentioned data loss.

The majority of the FTSE 100 also mentioned financial loss when discussing the potential results of cyber risk. We observed discussion of impact on revenue, profit, remedial costs and knock-on effects on cash flows. A substantial minority of reports cited potential penalties arising from regulatory non-compliance and other legal consequences, such as contractual damages or inability to meet contractual obligations. We have classified financial loss as distinct from theft or fraud leading to funds being misappropriated.

A few companies comment on the potential impact on the financial reporting process and the integrity of financial reporting, particularly in relation to the impact of IT systems failure.

The graph below groups the impacts that were identified, which included loss of assets (especially intellectual property for industries with advanced technologies, such as pharmaceuticals), increased environmental, health and safety risks (relevant to mining and oil and gas industries), poor product quality (most relevant to manufacturers), loss of licence (mentioned by media companies), restrictions to trade, impact on growth and adaptability.

Figure 4. Potential impact of cyber risk as described in FTSE 100 annual reports



A good example of describing the impact of the risk in relation to data security is presented by Worldpay Group plc, below:

PRINCIPAL RISK 5:

Data security

Movement in the year:

↑

↑

Link to strategy

We focus on understanding our customers in core market segments

page 42

We will realise the full potential of our business model

page 48

Financial loss and reputational damage due to a breach of confidential data or technology disruption caused by internal/external attack to Worldpay or third-party suppliers/merchants.

Risk appetite
Worldpay has no tolerance for the loss of, or otherwise unauthorised or accidental disclosure of, customer or other sensitive information. The operation of inadequate or ineffective security controls could expose Worldpay to the risk of violating statutory requirements and/or industry regulations, resulting in reputational damage and financial loss.

Risk indicators

- Number of attempted security breaches
- Number of security breaches
- Number of breaches to policy
- PEN testing results
- Ethical hacking results
- Number of identified security risks outstanding

Potential impacts

- The loss of, or otherwise unauthorised or accidental disclosure of, customer or other sensitive information could result in regulatory or legal sanctions and/or significant reputational damage
- Additional costs by way of compensation, litigation, fines and loss of sponsorship

Mitigants

- Worldpay operates multi-layer cyber security defences which are monitored for effectiveness and to ensure they remain current
- Extensive monitoring of attempts to breach the system takes place with detailed analysis to ensure all potential threats are identified and defensible

Actions in 2015

- Maintained Worldpay's PCI compliance groupwide and prepared for PCI v3.0
- Upgraded our core Data Centre DDoS (Distributed Denial of Service) protection and our US DDoS protection
- Additional anti Malware deployed into production
- Migrated Off Host applications/ services from RBS into Worldpay data centres

Worldpay Group plc 2015 Annual Report, p62

7

A company's own employees remain one of the biggest threats to cyber security, intentional or otherwise, but very few companies publicly acknowledge this fact. Education and culture are the best defences here

1.5 Did companies acknowledge all significant risks?

Although perhaps an unpalatable issue to discuss, in our experience and based on the current evidence, employees remain one of the biggest threats to cyber security and data loss as there are no completely reliable safeguards. Very few FTSE 100 annual reports identified their own employees as one of the threats to cyber security.

An example of disclosure on the topic of employee threat is provided by AstraZeneca, which refers to "intentional or inadvertent actions by our employees or vendors":

<p>Failure of information technology and cybercrime</p> <p>We are dependent on effective IT systems. These systems support key business functions such as our R&D, manufacturing, supply chain and sales capabilities and are an important means of safeguarding and communicating data, including critical or sensitive information, the confidentiality and integrity of which we rely on.</p> <p>Examples of sensitive information that we protect include loss of clinical trial records (patient names and treatments), personal information (employee bank details, home address), intellectual property of manufacturing process and compliance, key research science techniques, AstraZeneca property (theft) and privileged access (rights to perform IT tasks).</p> <p>The size and complexity of our IT systems, and those of our third party vendors (including outsource providers) with whom we contract, have significantly increased over the past decade and makes such systems potentially vulnerable to service interruptions and security breaches from attacks by malicious third parties, or from intentional or inadvertent actions by our employees or vendors.</p>		<p>Any significant disruption to these IT systems, including breaches of data security or cybersecurity, or failure to integrate new and existing IT systems, could harm our reputation and materially adversely affect our financial condition or results of operations.</p> <p>While we have invested heavily in the protection of our data and IT, we may be unable to prevent breakdowns or breaches in our systems that could result in disclosure of confidential information, damage to our reputation, regulatory penalties, financial losses and/or other costs.</p> <p>Significant changes in the business footprint and the implementation of the IT strategy, including the creation and use of captive offshore Global Technology Centres, could lead to temporary loss of capability.</p> <p>The inability to effectively backup and restore data could lead to permanent loss of data that could result in non-compliance with applicable laws and regulations.</p> <p>We and our vendors could be susceptible to third party attacks on our information security systems. Such attacks are of ever-increasing levels of sophistication and are made by groups and individuals with a wide range of motives and expertise, including criminal groups, 'hacktivists' and others. From time to time we experience intrusions, including as a result of computer-related malware.</p>
<p>AstraZeneca PLC Annual Report and Form 20-F Information 2015, p220</p>		

As recognition increases that the internal threat is significant, we expect to see more UK companies acknowledging the significant threat of employee action, intentional or otherwise (e.g. phishing emails) and explaining how the risk is managed or mitigated.

In this section, we look at whether the FTSE 100 demonstrate how seriously companies take ownership of cyber risk in the corporate governance statement. We focus attention on whether the board or a board committee is clearly leading the way and whether disclosures demonstrate that the board provides appropriate challenge to management.

2. Do boards demonstrate ownership?

2.1 Did boards take ownership of the risk in their annual report?

76% of FTSE 100 companies mentioned cyber security in the corporate governance statement – 11% fewer than identified cyber risk as one of their principal risks and uncertainties. Despite the executive and boardroom focus on this risk, our survey found that only 5% of FTSE 100 boards appear to have a director with direct specialist expertise. We looked for executive or non-executive directors described as having current or recent experience in cyber security, or in Chief Information Officer, Chief Technology Officer, Chief Information Security Officer or IT director roles. A handful of other boards mentioned information technology or digital skills in biographical details or skills tables, but without providing sufficient detail to conclude on the relevance of this experience. Digital and technology skills in the boardroom vary widely from company to company.

Most frequently, cyber security was mentioned as a matter covered by the audit committee (60%) or the risk committee (14 companies; 56% of those with a risk committee). In almost every case cyber security had not been identified specifically as a matter to be dealt with by one of these committees in the summary of their terms of reference provided in the annual report. The audit committee has the bandwidth and skills necessary to act as the catalyst driving the necessary increased focus on cyber risk and providing the challenge to management.

The level of audit committee disclosure on cyber risk was highly variable with many audit committee reports simply citing cyber security in a list of topics considered as part of internal financial control. In many cases, this does not add much to an investor's understanding of the board's interest in and ownership of the topic.

Some of the better disclosures include more than a passing comment regarding the focus of the board on providing suitable challenge to management in this area. For instance, they will mention the work performed or even a programme of continuous monitoring of cyber risk by the board itself or by a board committee. These programmes typically include the receipt of a regular report in relation to cyber security, regular updates from the Head of IT, arranged visits to IT security centres, meeting with external experts or obtaining and assessing external expert reports prepared on the company.

An extract from 3i's Audit and Compliance Committee report:

The Committee received two presentations in the year from the IT Director on cyber security risk management. Management engaged external advisers in late 2015 to assess the threat to cyber security, including the potential impact of cyber attacks, on both 3i's information and infrastructure and its portfolio companies. The Committee assessed the results of this review, including the proposed actions to strengthen risk management further, and were satisfied that 3i's capability was proportionate to its size and business activity. The Committee will receive an update on cyber security and the implementation of recommended actions in FY2017.

3i Group plc 2016 Annual Report, p76

“In the light of so many cyber events in the news, corporate boardrooms are beginning to understand the complexities and reputational risks they face; however for some there is still no clear ‘owner’ of this varied, often technical, and always complex issue. While many organisations may have a CISO, CTO or CIO there is often a lack of coherence in Board leadership with the right level of understanding, accountability or authority”

Dominic Cockram, Partner,
Regester Larkin by Deloitte

Our survey results showed that 39% of FTSE 100 boards and/or board committees disclose that they received at least one report on cyber security during the year. Just 18% disclose 'regular' receipt of updates to the Board and/or committees in relation to cyber security. Disclosed frequency of these 'regular' reports or updates varies from monthly to bi-annually.

The following example from Marks and Spencer Group plc includes commentary in the main corporate governance statement on the board's activity, followed by the audit committee's description of their activities around cyber security and business continuity.

ACTIVITIES/DISCUSSION	ACTIONS ARISING	PROGRESS
Conducted a review of the Company's cyber security position.	<ul style="list-style-type: none"> → Assess the strength of M&S's cyber security policies, capability and areas of risk. → Discuss the structure of our approach to cyber security in light of recent changes to data protection legislation. → Provide an objective assessment of business capabilities in light of the relevant risks. 	<ul style="list-style-type: none"> → Robust plans in place to ensure the business's cyber security systems remain sufficiently robust going forward. → Existing capabilities comprehensively reviewed and consideration given to future developments in the area of cyber security. → Areas of risk identified and future priorities agreed.
CYBER SECURITY <ul style="list-style-type: none"> → Updated on the cyber security measures in place at M&S, and noted the proactive approach adopted by the business. → Discussed the protection around customer data, including encryption and regular reviews of the security measures in place. → Updated on the external review of the company's cyber security systems, which were assessed against an external framework, and considered the proposed improvement plan. → Agreed regular updates be provided to the Committee throughout the year. 	BUSINESS CONTINUITY <ul style="list-style-type: none"> → Updated on progress made in the international business following the implementation of several initiatives, including the increased levels of crisis management training. → Discussed the current national threat level, level of preparedness with the introduction of shopping centre/retail park preparedness assessments, and key areas of improvement. → Discussed the strategy and focus for 2016/17 which includes international retail and sourcing, cyber security, and global terrorism. 	

Marks and Spencer Group Plc Annual Report and Financial Statements 2016, pages 36 and 44

3. Are mitigating activities well explained?

In this section, we look at how effectively FTSE 100 companies describe the management and mitigation strategies they apply to cyber risk, in particular:

- executive level responsibilities;
- contingency, crisis management or disaster recovery plans;
- IT policies;
- internal controls over cyber risk;
- systems testing;
- third party expertise, including external assurance; and
- other ways of mitigating or managing the risks, such as staff training, insurance and continuous monitoring.

The better disclosures mention clear ownership and reporting lines in relation to cyber security and regular board engagement

3.1 Do companies disclose who is responsible for cyber risk in the company?

One straightforward way that companies can demonstrate to investors that they take addressing cyber risk as a priority is to show they have thought about where responsibility lies at executive level, the reporting lines to the CEO and the board and whether a specialist non-executive director is needed.

The better disclosures mention clear ownership and reporting lines in relation to cyber security and regular board engagement.

11% of the FTSE 100 mentioned that they created a new role/body to have overall accountability for cyber risk during the previous year, demonstrating the increased focus on cyber risk in those organisations.

One company mentioned that an external cyber expert – neither a director nor an employee – attends board meetings, which is a way of ensuring the board has access to that expertise without adding a director with expertise in this area.

We observed that only 27% of FTSE 100 annual reports clearly identified a person or team with responsibility for cyber security.

Information technology
Executive responsibility: Chief Information Officer

- If information and data are not adequately secured and protected (data security, access controls), this could result in:
 - Increased internal/ external security threats
 - Compliance and reputational damages
 - Regulatory and legal litigation in case of failure to manage personal data
 - Reduced information accountability due to limited sensitive data access controls
- Utilise appropriate levels of industry-standard information security solutions for critical systems
- Continue to stay abreast of cyber-risk activity and, where necessary, implement changes to combat this
- Improved alignment between IT and business strategy

Hikma Pharmaceuticals Plc – Annual Report 2015, p56

The level of disclosure of policies and internal control activities over cyber needs improvement

3.2 What do companies disclose about contingency plans, crisis management or disaster recovery plans?

More than half of FTSE 100 companies mentioned contingency plans, crisis management or disaster recovery plans as a mitigating action for cyber risk. However, only just over half of these (58%) report that they had been tested during the year.

We expect that some companies did not take credit for having suitable plans in place and that plans are likely to be tested regularly. It would be helpful to stakeholders to understand that plans are in place and that they are tested, especially in sectors with a particularly high exposure to cyber risk in their operations.

We have also looked for the board’s involvement in assessing disaster recovery, crisis management or contingency plans in relation to cyber security, in particular involvement in how the scenario would be managed for reputation and business continuity purposes. However, we did not find any evidence of board involvement described in last year’s FTSE 100 annual reports – perhaps an area for consideration in future reports?

3.3 Do companies disclose internal controls and IT policies as ways of managing cyber risk?

We consider that all FTSE 100 companies would be expected by their investors and other stakeholders to have internal controls and IT policies in place to prevent IT security issues.

29% of FTSE 100 companies mentioned having internal policies in relation to cyber/data security as a mitigating factor. 8% of all companies mentioned review/update to or improvement in their internal policies in relation to cyber security during the year.

However, only 38% of companies mentioned internal controls in place as a mitigating factor in relation to cyber risk, and only 7% disclosed any changes to improve internal controls relating to cyber risk during the year.

Some disclosures discuss how they ensure and monitor adherence to group policies by their commercial partners, suppliers, contractors and what measures they have in place to protect their data and information technologies where third parties are involved, either through outsourcing or other arrangements.

Paddy Power Betfair plc talked about their internal controls as follows:

<p>Data Integrity and IT Security The integrity and security of our systems are key to the effective operation of the business and appropriate revenue recognition. As the Group regularly collects, processes and stores personal data through its business operations (including name, address, email, phone number and financial data such as bank details and betting history) it must ensure strict compliance with all relevant data protection and privacy related laws and regulations in all jurisdictions where it operates. The Group is potentially exposed to the risk that customer or employee personal data could be inappropriately collected, lost or disclosed, or processed in breach of data protection regulation. This could also result in formal investigations and / or possible litigation resulting in prosecution and damage to our brand and reputation.</p>	<p>The Group has appropriate data protection policies in place in order to protect the privacy rights of individuals in accordance with the relevant Data Protection legislation. The Group’s Legal and Compliance teams ensure the business adheres to industry best practice standards and relevant laws of data protection compliance. The Group has made significant investment in IT security resources and partners with a variety of external security specialists to ensure security arrangements and systems are up to date with emerging threats.</p> <p>IT security is embedded in IT operations and development processes. The Group’s Information and Security function continuously assesses the risks and controls around security and IT operations. The function reported to the Committee during the year. The specialist external IT auditor examined and tested the effectiveness of controls during the audit. Based on assurances from management and the external auditor the Committee is satisfied with internal controls and the residual level of risk.</p>
---	--

Paddy Power Betfair plc Annual Report 2015, p54

Both a policy framework and internal controls are important forms of mitigation in terms of cyber security, however because of the pace of evolution and increasing sophistication of cyber threats we would ordinarily expect other measures to be in place to mitigate cyber risk and encourage companies to disclose these additional measures to improve their disclosures.

3.3 Do companies disclose other forms of management or mitigation?

In our experience, larger companies will generally have all or most of the management or mitigation strategies above: someone who deals with cyber risk, a policy framework, internal controls and disaster recovery plans. However there are other effective ways of targeting cyber risk which can help to offer additional confidence to investors and other stakeholders. We surveyed the FTSE 100 to see what types of other targeted measures they disclosed.

Staff training

28% of FTSE 100 companies mentioned delivering staff training in relation to cyber risk during the year and 10% of companies mentioned that cyber related training had been delivered to the board.

Insurance

5% of FTSE companies mentioned insurance against cyber risk – something cyber professionals believe has become critical.

Systems testing

22% of the FTSE 100 mentioned that some form of vulnerability testing³, penetration testing⁴ or other cyber risk specific testing had been performed during the year. This is particularly helpful disclosure as it demonstrates that the company has a way of identifying and addressing flaws in their existing protections and that it is committed to fixing those flaws.

Other targeted measures included training for staff and the board, cyber insurance, external assurance, systems testing and continuous monitoring of systems and vulnerabilities

³ Vulnerability testing is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure

⁴ Penetration testing is the practice of simulating how an attacker might try to exploit vulnerabilities in a computer system, network or Web application

External assurance or assistance

Just 9% of the FTSE 100 disclose external assurance activities in relation to cyber risk. One company mentioned ISO certification (ISO27001) and another mentioned a less specific ‘internationally recognised certification’ as a mitigating factor.

Continuous monitoring

Another management strategy disclosed was the use of global 24/7 security operations monitoring centres, demonstrating the level of importance and the level of control those companies maintained in relation to cyber security. Easyjet mentioned ‘quarterly vulnerability scanning’, which is a good example of a clear disclosure of continuous monitoring.

Examples

Good examples of disclosure of principal risks, including management or mitigation strategies, are specific to the business and tell investors and other stakeholders the key things they need to know. We consider that, along with the other examples provided in this publication, it’s worth taking a look at the disclosures provided by Wolseley Group plc, Experian plc and BT Group plc (below).

Security and resilience

Resilient IT systems, networks and associated infrastructure are essential to our commercial success. There are a lot of different hazards that could significantly interrupt our services.


These include the evolving threat of cyber-attack, as hackers increasingly see Internet Service Providers (ISPs) as attractive targets. Others include component failure, physical attack, copper cable or equipment theft, fire, explosion, flooding and extreme weather, power failure, overheating or extreme cold, problems encountered during upgrades and major changes, and suppliers failing to meet their obligations.


Potential impact

A malicious cyber-attack or breach of security could mean our data is lost, corrupted, disclosed or ransomed, or that our services are interrupted. We might have to pay fines, contract penalties and compensation, and have to operate under sanctions or temporary arrangements while we recover and put things right.

A big interruption to our services, from cyber-attack or otherwise, could mean immediate financial losses from fraud and theft; contract cancellations; lost revenue from not being able to process orders and invoices; contractual penalties; lost productivity and unplanned costs to restore and improve our security; prosecution and fines. Ultimately individuals’ welfare could be put at risk where we weren’t able to provide services or personal data was misappropriated.

Our revenues, new business and cash flow could suffer, and restoring our reputation and re-building our market share might take an extended period of time.


Link to strategy and business model

- Deliver superior customer service Trend: 

What’s changed over the last year?

We’ve invested in scanning and monitoring tools and automated cyber defences. But the rate of major cyber-related incidents needing a manual response keeps rising. We’ve increased the size of our Cyber Defence Operations team accordingly. To probe for vulnerabilities they simulate cyber-attacks. When we learn of potential attack routes, or get intelligence about attacks on similar organisations, we treat the information proactively and resolve it with the same speed and rigour as a real attack.

We’ve reviewed the resilience and disaster recovery capability of our critical systems, main data centres and our most important exchanges. This has helped us make judgements on where to invest in better and stronger systems and infrastructure. We’re also continuing to develop cross-site recovery for our critical systems where this didn’t previously exist. There are also several major change programmes underway to intensify IT and network controls to meet new levels of risk.

How we’re mitigating the risks

We use encryption to prevent unauthorised access to data travelling over our networks, or through direct access to computers and removable storage devices.

But encryption alone can’t eliminate this risk. People can be tricked into downloading malware or giving away information by phone or email. So we also implement extra layers of access control, block as many malicious emails as we can, and run awareness campaigns for customers and employees to make sure they stay vigilant.

We ask suppliers for evidence of compliance with our security policies. We also run an audit programme to test this. We simulate cyber-attacks to test how well protected our websites, networks and internal controls are.

A control framework helps us prevent service interruptions, supported by tried and tested recovery capabilities. Proactive problem management helps us address the root causes of common incidents.

We continue to invest in resilience and recovery capabilities for critical IT systems, as well as addressing vulnerabilities in our physical estate as we become aware of them. We also have a rolling programme of major incident simulations to test and refine our procedures for crises.

By replacing equipment approaching the end of its service life, we’re moving more of our legacy estate to new, more resilient facilities. We’ve also made sure that we have geographically-distributed locations that support cross-site recovery.

BT Group plc Annual Report and Form 20-F 2016, p49

4. Are cyber security breaches described?

In this section, we look at whether FTSE 100 companies describe their experience of cyber breaches and how they have addressed the challenge of disclosure.

4.1 Did companies disclose cyber security breaches?

Almost all companies experience some degree of cyber security breach reasonably regularly. However, not all of these are sufficiently significant that they will become public knowledge.

We observed that most of the FTSE 100 mentioned an increase in cyber security breaches in their industry, however substantially fewer (10%) cited cyber security incidents in their organisation. Two of those ten, both within the financial services sector, mentioned 'distributed denial of service' (DDoS) attacks. This type of attack often causes temporary business disruption due to complete or partial failure of IT systems.

Six companies specifically mentioned other types of cyber crime, including theft of intellectual property (one company), data security breaches (two companies, one including unauthorised access to a server with consumers' personal data). Companies also mentioned computer viruses and other malware, phishing, disruptive software attacks, and advanced persistent threats.

An example of disclosing a cyber breach but ensuring the focus is on the company addressing risks going forward is below:

A 2016 Register Larkin survey showed that almost half of corporate communication teams did not have a cyber communications plan or guidelines in place for a cyber incident. This further underlines the need for board level focus

Information protection	
<p>Risk definition Failure to protect and maintain access to critical or sensitive computer systems or information.</p> <p>Risk impact Failure to adequately protect critical and sensitive systems and information may result in loss of commercial or strategic advantage, damage to our reputation, litigation, or other business disruption including regulatory sanction, which could materially and adversely affect our financial results.</p> <p>Context We rely on critical and sensitive systems and data, such as corporate strategic plans, sensitive personally identifiable information, intellectual property, manufacturing systems and trade secrets. There is the potential that malicious or careless actions expose our computer systems or information to misuse or unauthorised disclosure.</p> <p>Several GSK employees were indicted for theft of GSK research information. While the charges against the individuals are concerning, based on what we know, we do not believe this breach has had any material impact on the company's R&D activity or ongoing business. GSK is conducting a full internal review into what occurred, and planning to continue to enhance the multiple layers of data protection that we already have in place.</p>	<p>Mitigating activities The Group has a global information protection policy that is supported through a dedicated programme of activity. To increase our focus on information security, the Group established the Information Protection & Privacy function to provide strategy, direction, and oversight while enhancing our global information security capabilities.</p> <p>We assess changes in our information protection risk environment through briefings by government agencies, subscription to commercial threat intelligence services and knowledge sharing with other Pharmaceutical and cross-industry companies.</p> <p>We aim to use industry best practices as part of our information security policies, processes and technologies and invest in strategies that are commensurate with the changing nature of the security threat landscape.</p> <p>We are also subject to various laws that govern the processing of Personally Identifiable Information (PII), the Group's Binding Corporate Rules (BCRs) have been approved by the UK Information Commissioner's Office for human resource and research activities data. BCRs have been signed by 23 European states allowing us transfer PII internationally between the Group's entities without individual privacy agreements in each European Union country.</p>

GlaxoSmithKline plc Annual Report 2015, p239

A 2016 Register Larkin survey showed that almost half of corporate communication teams did not have a cyber communications plan or guidelines in place for a cyber incident. This further underlines the need for board level focus.

5. Professional guidance

In the absence of a specific UK cyber disclosure framework the SEC Guidance provides information investors would expect

Cyber risk is a risk worldwide and a patchwork of guidance is emerging.

EU regulation, including the upcoming Directive on security of network and information systems (NIS directive) and the General Data Protection Regulation (GDPR) will require disclosure to monitoring organisations around cyber incidents, but this will not necessarily have a knock-on effect to public reporting.

There is some specific guidance and new plans in the USA and we expect the expectations from UK regulators and investors around disclosure only to increase in this area.

5.1 Disclosure guidance

There is no specific disclosure guidance in the UK, although both investors and the FRC have mentioned cyber risk as one risk that should be considered when reporting on principal risks and uncertainties.

In the USA, there is existing guidance on disclosures around cybersecurity. The Securities and Exchange Commission (SEC) Division of Corporate Finance issued disclosure guidance as far back as 2011, reminding registrants of their existing responsibilities and helping to tailor advice to the particular challenges of cyber. The guidance takes pains to point out that disclosure is not expected to provide a roadmap that could expose features of the company's cybersecurity and put it at risk.

5.2 Cyber risk management and related controls

Currently, there is no single approach for reporting to stakeholders on an entity's cyber risk management program and related controls designed to meet the needs of a broad range of users (i.e. boards, existing and prospective customers, suppliers, regulators, investors, analysts).

In response the AICPA in the USA is currently formulating a cybersecurity examination engagement, intended to expand cyber risk reporting to address the marketplace need for greater stakeholder transparency. The idea is to provide a broad range of users with information about an entity's cyber risk management programme that would be useful in making informed decisions. This proposed reporting mechanism would consist of:

- a description of the entity's cyber risk management programme; and
- an assessment of the effectiveness of the controls that are part of the programme.

Key features of the SEC guidance include:

- inclusion of cyber risk as a risk factor, where relevant, having considered the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks;
- adequately describing the risk, which could include;
 - discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
 - to the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
 - description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
 - risks related to cyber incidents that may remain undetected for an extended period;
 - description of relevant insurance coverage; and
 - disclosure of known or threatened cyber incidents to place the risk in context – this encourages discussion of specific real events rather than theoretical events;
- management’s discussion and analysis should include description of material events, trends or uncertainties relating to cyber risk, including those arising from actual incidents;
- disclosure of the impact of cyber incidents on particular business segments or future viability; and
- discussion of deficiencies in disclosure controls and procedures identified through management’s assessment of the effectiveness of those controls.

Further resources

This section pulls together additional resources that may be useful as a deeper dive on governance topics of interest, or which we believe can add insight on cyber risk and the impacts that can be associated with it.

As always, do get in touch with your Deloitte partner or with us in the Deloitte governance team if you would like to discuss any areas in more detail. All our governance publications are available to read and download from www.deloitte.co.uk/governancelibrary.

External resources – UK



FRC's letter to audit committee chairs and finance directors on summary of key developments for 2016 annual reports.



Audit insights: cyber security – Closing the cyber gap (ICAEW Information Technology Faculty publication).



Audit insights: cyber security – Taking control of the agenda (ICAEW Information Technology Faculty publication).

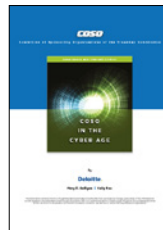


Article: Nearly half of communication teams feel unprepared to communicate about a cyber incident.

External resources – USA



AICPA cyber security resource centre, including links to exposure drafts referred to in this report.



COSO in the cyber age.



SEC disclosure guidance on cybersecurity.

Governance in Brief



Cyber risk – how are boards responding? explores the results of the third annual FTSE 350 UK Cyber Governance Health Check run by UK government and provides insights into how boards are strategically managing and responding to cyber risk.



EU Privacy Legislation explores the recent issues with transfer of data between the EU and the US and the existing solutions, the EU General Data Protection Regulation (GDPR) which is set to be enforced from 25 May 2018, and includes a series of questions to consider when determining how well prepared your organisation is for the upcoming changes.

Other recommended Deloitte publications



Beneath the surface of a cyberattack: a deeper look at business impacts questions whether leaders accurately gauge the impact a cyberattack can have on their organisation and whether common assumptions about the costs and recovery process associated with data breaches paint a clear picture. It considers, in financial terms, the broad and extended business impact of cyberattacks, including both direct and intangible costs.



Risk appetite: Is your disclosure where you want it? presents a pragmatic, multi-stage approach to risk management and determining risk appetite, outlining the key content for each stage and concluding with a range of key questions for boards to consider.



Focus on: The board's-eye view of cyber crisis management discusses the potential effects of a cyber breach. It looks at the role the board plays in helping organisations determine how to respond to the new cyber threat landscape, the six different types of crisis triggers for which most organisations should be prepared, and what steps your board needs to take to ensure risk sensitive assets are secured.



Reputation matters: Developing reputational resilience ahead of your crisis identifies two fundamentals in building reputational resilience – identification of risks from an outside in perspective, and being prepared for a crisis through a robust crisis readiness programme. Looking ahead, it will be the organisations that understand, protect and develop their reputation asset that will be best placed to maintain shareholder value.



Cybersecurity and the role of internal audit highlights the critical role of internal audit in the ongoing battle of managing cyber threats, both by providing an independent assessment of existing and needed controls, and helping the audit committee and board understand and address the diverse risks of the digital world.

Appendix: How to disclose cyber risk

Some ideas to help you enhance reporting on cyber risk in the annual report

We include below ideas based on areas of reporting we identified from completing this first survey covering cyber risk reporting across all FTSE 100 annual reports. It can provide inspiration for improved disclosures on cyber risk in your annual report.

Ideas	Y/N
Describing cyber risk	
1. Have you included cyber risk as a principal risk in your strategic report?	
2. Have you considered the key areas of exposure for your industry/company and disclosed each one that represents a principal risk: <ul style="list-style-type: none"> • Cyber crime • IT systems failure • Data protection • Data theft or misappropriation 	
3. Have you thought about and correctly categorised each cyber risk and how cyber risk most affects your industry/company? <p><i>Note: Most FTSE 100 companies in our survey presented cyber risk within operational risks category.</i></p>	
4. Have you disclosed changes to the principal risk(s) associated with cyber since the previous year: <ul style="list-style-type: none"> • Change in likelihood • Change in potential impact • Change in potential timing <p><i>Note: The better disclosures we saw acknowledged and explained an increase in cyber risk irrespective of the amount and quality of mitigating actions due to the increasing sophistication of cyber criminals.</i></p>	
5. Have you disclosed specific types of cyber crime that you have experienced or expect to be exposed to: <ul style="list-style-type: none"> • Unauthorised access • Hacking or hacktivists • Malware, including computer viruses • Distributed denial of service (DDOS) attacks • Targeted fraud attacks, including phishing attacks • Terrorism related attacks • Geopolitical cyber threats, including threat of attack by foreign governments 	
6. Have you clearly disclosed the threat posed by employee action or inaction?	
7. Have you disclosed any cyber threats in relation to commercial partners, suppliers, contractors and other third parties?	
8. Have you clearly disclosed the potential impact if identified cyber risks were to crystallise: <ul style="list-style-type: none"> • Financial implications (including impact to revenue, profit, cash flows, any remedial costs, financial fraud) • Disruption to business/operations • Loss of commercial or strategic advantage • Loss of or detriment to client or contract • Reputational damage, including loss of investor or stakeholder trust • Legal implications (inability to meet contractual obligations, regulatory non-compliance and penalties, contractual damages) • Impact to the integrity of the financial reporting process • Misappropriation of funds or assets • Loss of intellectual property 	

Ideas	Y/N
Board ownership	
9. Do you talk about cyber risk in the corporate governance section of the annual report?	
10. Do you talk about cyber risk in the audit or risk committee sections of the annual report, and if cyber risk monitoring has been delegated to a board committee, is the split of responsibilities clearly explained?	
<i>Note: In our view, in most companies the audit committee will be the catalyst driving the necessary increased focus on cyber risk and applying challenge to management.</i>	
11. Where you discuss the board or board committee involvement, is there evidence of understanding, education and challenge?	
12. Is board level responsibility for cyber risk acknowledged and any designated board member identified?	
13. Where an individual or team below board level leads on cyber risk, is that clearly disclosed with a direct reporting line to the board described?	
Mitigating cyber risk	
14. Have you disclosed contingency plans, crisis management or disaster recovery plans that form part of cyber risk mitigation? If yes, have you disclosed whether these plans are tested regularly (preferably at least annually)?	
15. Have you disclosed IT or cyber policies in place to manage cyber risk, together with any updates or reviews during the last year?	
16. Have you disclosed the existence of key internal controls in place to manage cyber risk, together with any relevant improvement or review in the last year?	
17. Have you discussed how you monitor the adherence to your company's IT security policies by your commercial partners, suppliers, contractors?	
18. Have you discussed any measures you have in place to protect your data and information technologies where a third party is involved, either due to outsourcing or other arrangements?	
19. Have you mentioned staff training or awareness programmes in relation to cyber security?	
<i>Note: Better FTSE 100 annual reports also mention cyber security training provided to the Board.</i>	
20. Have you mentioned insurance in relation to cyber security (if any)? If so, have you disclosed which exposures are covered by cyber insurance?	
21. Have you mentioned systems testing, such as penetration testing, vulnerability testing or other cyber risk specific testing that has taken place during the year?	
22. Have you mentioned engaging external assurance or other external advice to mitigate cyber risk? If so, it is helpful to be specific regarding which external parties you have engaged with or what services have been obtained.	
23. Have you disclosed any certification regarding cyber security (ISO or equivalent)?	
24. If you use security operations monitoring centres to monitor cyber security full time, has this been disclosed?	
25. Are there any other relevant mitigating actions that could usefully be disclosed?	
Disclosing cyber security breaches	
26. Have you disclosed any cyber security breaches experienced during the year? If so, have you explained any remediating actions taken or controls put in place?	

Contacts

Risk advisory: cyber risk

If you would like to contact a specialist in cyber risk regarding any matters in this report, please use the detail provided below:



Phill Everson

Tel: +44 (0) 20 7303 0012

Email: peverson@deloitte.co.uk



Stephen Bonner

Tel: +44 (0) 20 7303 2164

Email: stephenbonner@deloitte.co.uk

Regester Larkin by Deloitte

Regester Larkin by Deloitte advises on high impact strategic risks and managing uncertainties, crises and issues, whether as a result of geopolitical, economic, financial, or cyber-related events or through corporate misdeed or high impact operational or technological failures. They also provide forensic, cyber response, claims management, regulatory and financial restructuring expertise through Deloitte's cross-firm crisis management risk advisory practice.



Rick Cudworth

Tel: +44 (0) 20 7303 4760

Email: rcudworth@deloitte.co.uk



Dominic Cockram

Tel: +44 (0) 20 7303 2288

Email: dcockram@deloitte.co.uk

The Deloitte Centre for Corporate Governance

If you would like to contact us please email corporategovernance@deloitte.co.uk or use the details provided below:



Tracy Gordon

Tel: +44 (0) 20 7007 3812
Mob: +44 (0) 7930 364431
Email: trgordon@deloitte.co.uk



Corinne Sheriff

Tel: +44 (0) 20 7007 8368
Mob: +44 (0) 7824 609772
Email: csheff@deloitte.co.uk



William Touche

Tel: +44 (0) 20 7007 3352
Mob: +44 (0) 7711 691591
Email: wtouche@deloitte.co.uk

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training. Membership of the Deloitte Academy is free to board directors of listed companies, and includes access to the Deloitte Academy business centre between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website www.deloitteacademy.co.uk which members can use to register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including membership, please email enquiries@deloitteacademy.co.uk.





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2017 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000
Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. J10985