Deloitte.

Governance in focus

Cyber risk reporting in the UK

March 2018

Contents

This survey covers FTSE 100 annual reports for the most recent year end as at 30 September 2017.
Comparative period analysis drawn from our previous survey is described as 2017 data.

Reporting on cyber risk

Foreword from William Touche

Dear Public Company Director,

This survey represents our second review of cyber reporting by the UK's FTSE 100, designed to help you identify examples of good practice and to offer insight about how to keep the users of annual reports informed.

In summary: progress has been made. Companies are talking about cyber risk more and are including more detail about governance structures and mitigation. This year 99 out of 100 companies mention cyber risk.

However, a substantial majority of companies are still not reporting that they receive and deal with cyber attacks. Companies should consider whether this is somewhat disingenuous – after all, investors, regulators and the informed public are well aware that companies will regularly be fending off cyber attacks of varying degrees of sophistication.

Key to disclosures on cyber risk and other complex or long term risks is building trust between the company, its shareholders and its wider stakeholder community. This means transparency of disclosure. This trust, once established, is a powerful tool to build reputation and customer loyalty.

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 let 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, how they report to the board, 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 Appendix 1.
- 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.

Of course, privacy and data protection is a hot topic at the moment as the General Data Protection Regulation (GDPR) comes into force on 25 May. We have not focused on company disclosures on their progress in implementing this regulation as it is frequently identified as a regulatory risk, as opposed to a technology-related risk.

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.

At a glance

- 99% of the FTSE 100 mentioned cyber risk (2017: 95%).
- 89% clearly pulled out one or more types of cyber risk as a principal risk in their disclosures (2017: 87%).
- The most common impacts disclosed were the potential disruption of business/ operations 70% (2017: 68%), data loss 58% (2017: 45%) and reputational damage 56% (2017: 58%).
- 23 companies acknowledged employee risk as one of the biggest threats to cyber security and data loss, a significant increase compared to 2017.
- 8% of board disclosures indicate that there is a director on the board with direct specialist expertise (2017: 5%).
- 58% mentioned contingency plans, crisis management or disaster recovery plans as a mitigating action for cyber risk. Only just over half of these reported that these plans had been tested during the year – and only two boards disclosed oversight responsibilities for these plans.
- Only 8% mentioned insurance against cyber risk (2017: 5%) – something cyber professionals believe has become critical.
- Only 11% (2017:10%) cited cyber security incidents in their organisation. Transparency on this topic is key to building long term trust.

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.

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

89% of the FTSE 100 clearly pulled out one or more elements of cyber risk as a principal risk in their disclosures (2017: 87%).

1.1 Did companies recognise cyber risk as a principal risk?

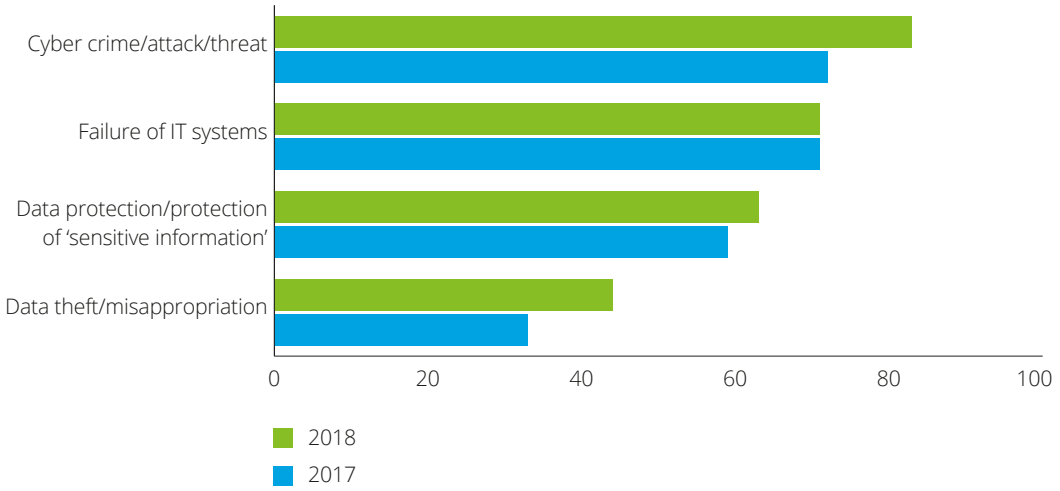
We started by analysing how cyber risk was reported in the annual report of each FTSE 100 company.

89% of the FTSE 100 clearly pulled out one or more elements of cyber risk as a principal risk in their disclosures (2017: 87%).

Companies disclosed four types of 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. In our opinion the better disclosures incorporated discussion of all key cyber risk elements.

Although a majority of these companies (47 companies or 53%) also mentioned that the risk had increased compared to the previous year, this was lower than the prior year, when 56 companies mentioned that the risk had increased (64%).

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



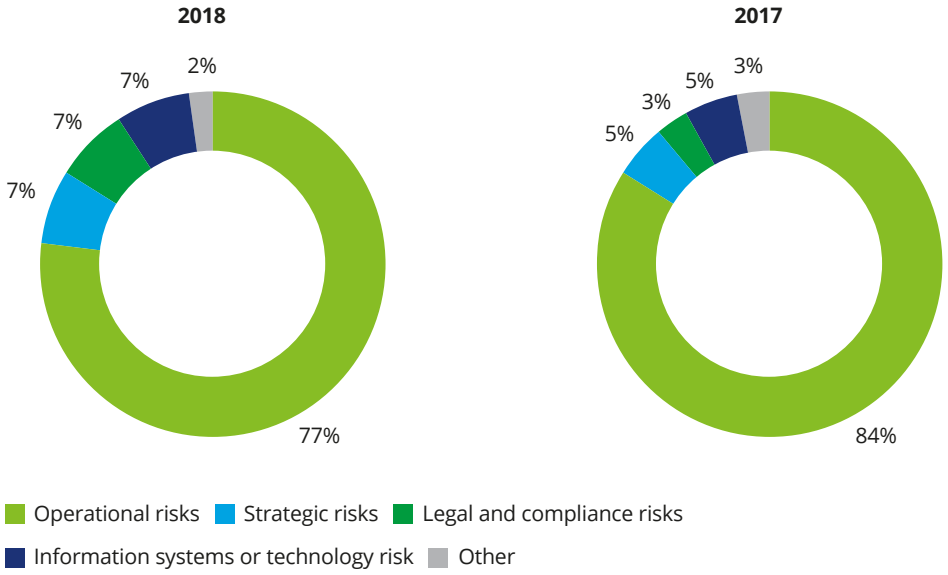
For almost half of the FTSE 100 to call data theft out as a principal risk indicates just how reliant we all are on technology, and how this increases our vulnerability.

Cyber crime or cyber attack was identified as an aspect of the principal risk by 83%, a substantial increase from 72% in 2017. IT systems failure was identified in the principal risks disclosure by 71% of the FTSE 100.

We define data protection risk as the risk around sensitive information, in particular compliance with data protection regulations. This was called out by 63% (2017: 59%) of companies, while data theft or misappropriation of data, including intellectual property (IP) was specifically identified as a further risk in addition to cyber crime in 44% of annual reports, up from 33%.

For almost half 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.

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



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

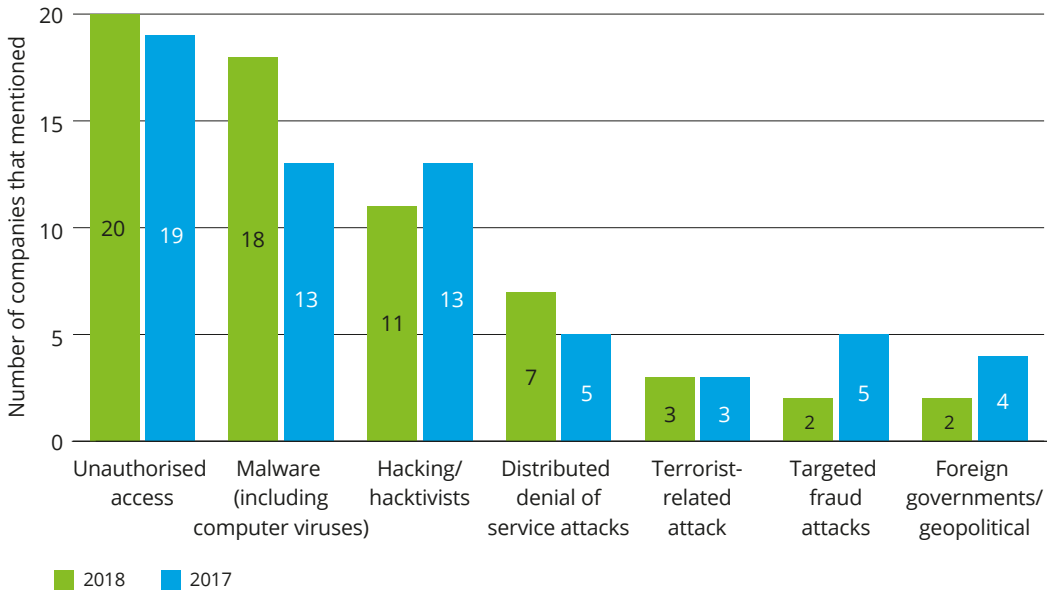
Most of the companies that categorised their principal risks (30 of the FTSE 100) recognised cyber risk as part of operational risk.

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

1.2 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. Figure 3 explains the nature of the cyber crime mentioned by the 83 companies that identified cyber crime as an aspect of their principal risk.

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



Although unauthorised access to systems is a threat faced by all companies with digital assets, only 20% mention that threat.

It is immediately obvious that companies do not have a consistent approach to calling out the types of cyber crime they face. For instance, although unauthorised access to systems is a threat broadly faced by all companies with digital assets, only 20% (2017: 19%) mention that threat.

There is a broad spread of other threats mentioned by companies, notably the threat of malware (including computer viruses), which rose to 18% compared to 13% in the previous year, and hacking and/or hacktivists at 11% (2017: 13%). It was more common to see specifics about the types of cyber crime faced from companies in the financial services sector.

This year one FTSE 100 annual report also identified the risk of damage to brand reputation due to adverse comment on social media regarding cyber breach or data loss.

1.3 How did companies describe the impact of cyber risk?

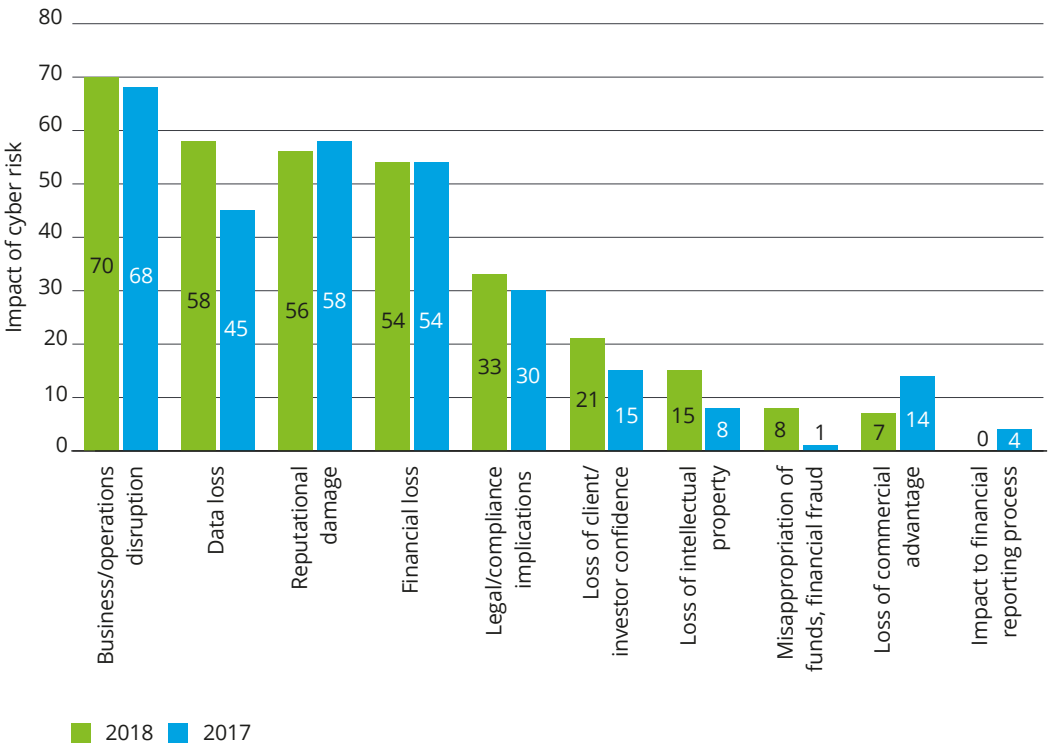
The most common impact, mentioned by 70% of the FTSE 100, was the potential disruption of business/operations, 58% mentioned data loss (up from 45% last year) and 56% mentioned reputational damage.

The majority of the FTSE 100 also mentioned financial loss when discussing the potential impact 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.

A few companies commented 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. This year one FTSE 100 annual report also identified the risk of damage to brand reputation due to adverse comment on social media regarding cyber breach or data loss.

We have classified financial loss as distinct from theft or fraud leading to funds being misappropriated.

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



Some companies also mentioned cyber risk in relation to the potential impact on their ongoing viability, which they disclosed in their viability statements, with examples of disclosure including descriptions of potential information security scenarios.

Impact of cyber risk on ongoing viability has been disclosed by some companies in their viability statements, describing information security scenarios.

1.4 Did companies acknowledge employee risk?

Although there is debate in the cyber security community as to whether employees are responsible for their role as one of the biggest threats to cyber security and data loss, or whether this is instead due to underlying poor security design, the fact remains that there are no completely reliable safeguards to employee risk. Last year very few companies acknowledged this in their annual reports.

This year we identified a substantial increase in the number of annual reports identifying a significant internal threat – now 23 of the FTSE 100 – generally commenting on employees or contractors. This is encouraging as it indicates that understanding of the threat environment at a senior level is moving on.

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.

1.5 Did companies acknowledge third party risk?

Another challenging area where we have seen more and clearer disclosure this year is in third party risk – the risk that a supplier, or even a customer, who interacts with a company's systems, may open that company to unauthorised access.

2. Do boards demonstrate ownership?

Only 8% of FTSE 100 boards appear to have a director with direct specialist expertise. This year we have seen some FTSE 100 boards being more open about the need for cyber expertise on the board.

It is useful to explain how matters considered at committee level have been pulled together into a comprehensive response at board level.

In this section, we look at whether the FTSE 100 demonstrate how seriously their boards 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.

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

79% of FTSE 100 companies mentioned cyber security in the corporate governance statement (2017: 76%). This compares to 89% that 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 8% of FTSE 100 boards (2017: 5%) appear to have a director with direct specialist expertise.[1] A handful of other boards mentioned information technology or digital skills in board member biographical details or skills tables, but without providing sufficient detail for us to conclude on the relevance of this experience.

This year we have seen some FTSE 100 boards being more open about the need for cyber expertise on the board.

Better disclosures in the corporate governance statement around cyber risk include detail regarding the focus of the board on providing suitable challenge to management in this area. For instance, they mention the work performed or even a programme of continuous cyber risk monitoring by the board 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, meetings with external experts, and obtaining and assessing external expert reports prepared on the company.

It is useful to explain how matters considered at committee level have been pulled together into a comprehensive response at board level.

45% of FTSE 100 boards and/or board committees disclosed that they received at least one report on cyber security during the year (2017: 39%). Just 21% disclosed 'regular' receipt of updates to the Board and/or committees in relation to cyber security (2017: 18%). Disclosed frequency of these 'regular' reports or updates varies from monthly to bi-annually.

2.2 Did boards disclose detail about the governance of cyber risk in their annual report?

Cyber security was mentioned as a matter covered by the audit committee (58%; 2017: 60%) or the risk committee (16 companies compared to 14 companies in 2017). In one case this year an audit committee terms of reference summary in the annual report referred to cyber security.

1 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.

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. Clearly, this does not add much to an investor's understanding of the board's interest in, and ownership of, an important topic.

8% of FTSE 100 companies disclosed that they have a Chief Information Security Officer (CISO) as part of the executive team. In most cases this is in the context of the CISO being a member of executive committees focusing on cyber security and reporting into the Board, for instance a group risk or data governance committee. One company disclosed that the CISO regularly meets with and briefs the audit committee, an example of clear governance structures in cyber security.

Some companies helpfully disclose more detail about the governance model applied to cyber risk throughout the organisation, although in some cases this is a brief mention of the structure applied. For instance, one company talks about moving the CISO function into the risk and compliance function, but without providing further detail on why or how the governance model would work.

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.

8% of FTSE 100 companies disclosed that they have a Chief Information Security Officer (CISO) as part of the executive team.

3. Are mitigating activities well explained?

Almost one in five FTSE 100 companies has revisited the governance around cyber and data risk over the past two years – a good indication of how seriously these organisations take the risk

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.

3.1 Do companies disclose who is responsible for cyber risk?

One straightforward way that companies can demonstrate to investors that addressing cyber risk is 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.

7% of the FTSE 100 mentioned that they created a new role/body to have overall accountability for cyber risk during the previous year. This compares to 11% in our 2017 report, meaning that almost one in five FTSE 100 companies has revisited the governance around cyber and data risk over the past two years – a good indication of how seriously these organisations take the risk.

We observed a noticeable increase in disclosed responsibility for cyber security this year. 38% of the FTSE 100 (2017: 27%) clearly identified a person or team with responsibility for cyber security.

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 (57%) reported that these plans 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 investors and other stakeholders to understand that plans are in place and that they are tested regularly, 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 a scenario would be managed for reputation and business continuity purposes. Whilst last year we did not find any evidence of board involvement in disaster recovery plans in the annual reports, this year two companies put their hands up to explain that the board or a committee has oversight of this process. This is a topic companies should consider in future reports.

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

All FTSE 100 companies would be expected by their investors and other stakeholders to have internal controls and IT policies in place to manage IT security issues.

38% of FTSE 100 companies mentioned having specific policies in relation to cyber/data security as a mitigating factor (2017: 29%). 14% of companies mentioned review/update to, or improvement in, their policies in relation to cyber security during the year.

Over half of companies mentioned internal controls in place as a mitigating factor in relation to cyber risk, and 31% disclosed changes to improve internal controls relating to cyber risk during the year. This is a substantial change from the previous year, where only 38% discussed internal controls and only 7% mentioned changes to those internal controls – a real improvement in disclosure.

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 (57%) reported that these plans had been tested during the year.

3.4 Do companies disclose other forms of management or mitigation?

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

Staff training

31% of FTSE 100 companies mentioned delivering staff training in relation to cyber risk during the year (2017: 31%) and 12% of companies mentioned that cyber related training had been delivered to the board (2017: 10%).

Insurance

8% of FTSE 100 companies mentioned insurance against cyber risk (2017: 5%) – something cyber professionals believe has become critical.

Some FTSE 100 companies mention that cyber insurance is covered under their policies for general business continuity insurance.

Systems testing

20% of the FTSE 100 mentioned that some form of vulnerability testing, penetration testing, "ethical hacking"[2] or other cyber risk specific testing had been performed during the year (2017: 22%). 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.

External assurance or assistance

Just 7% of the FTSE 100 disclose external assurance activities in relation to cyber risk (2017: 9%). Four companies mentioned ISO certification (ISO27001) as a mitigating factor (2017: one company).

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 regular monitoring.

Examples

Good disclosures of principal risks, including management or mitigation strategies, should be specific to the business and tell investors and other stakeholders the key things they need to know.

2 Ethical hacking is the exercise of testing companies' cyber security in the same way as a malicious hacker would test it, but with the ethically sound goal of improving the company's security.

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.

Most of the FTSE 100 mentioned an increase in cyber security breaches in their industry, however substantially fewer (11%; 2017: 10%) cited cyber security incidents in their organisation. Only three of these included more detail than a brief mention of experiencing attacks of various sorts.

Tesco Bank discloses a cyber breach and ensures that the focus of the disclosure is on the company addressing the risk going forward. The Chairman also briefly discussed the breach in his statement elsewhere in the annual report.

Tesco Bank		
Tesco Bank is exposed to a number of risks, the most significant of which are credit risk, operational risk, liquidity and funding risk, market risk, and legal and regulatory compliance risk. 1	The Bank continues to actively manage the risks to which it is exposed.	The Bank has a defined risk appetite which is approved and reviewed regularly by both the Bank's Board and the Tesco PLC Board. The risk appetite defines the type and amount of risk that the Group is prepared to accept to achieve its objectives and forms a key link between the day-to-day risk management of the business, its strategic priorities, long-term plan, capital planning, liquidity management and stress testing. Adherence to risk appetite is monitored through a series of ratios and limits. The Bank operates a risk management framework that is underpinned by governance, policies, processes and controls, reporting, assurance and stress testing. There is Bank Board risk reporting throughout the year, with updates to the Tesco PLC Audit Committee by the Bank CFO/Audit Committee Chairman. A member of the Tesco PLC Board is also a member of the Bank's Board. In November 2016, Tesco Bank's debit cards were the subject of an online fraudulent attack. The Group's priority throughout was to ensure customers' accounts were protected and that it communicated with customers immediately and transparently, reassuring customers that there was no data loss or breach of systems. The Group has undertaken immediate remedial action and an independent review of the issue and continues to work closely with the authorities and regulators on this incident.

Most of the FTSE 100 mentioned an increase in cyber security breaches in their industry, however substantially fewer (11%) cited cyber security incidents in their organisation.

5. Professional guidance

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

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

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 competent authorities around cyber incidents, but this will not necessarily include public reporting.

There is some specific guidance and new plans in the USA and it is likely that expectations from UK regulators and investors around disclosure will only 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.

The FRC's draft updated Guidance on the Strategic Report calls upon boards to consider non-financial as well as financial risks. It also mentions the importance of explaining potential changes to the strategy and business model arising from long-term systemic risks which may have a material effect on the entity's ability to generate and preserve value, which for some companies may include risks arising from changing technology.

The draft Guidance also uses cyber risk as an example of disclosure on changes in the risk profile of an entity. It explains that risk disclosures should identify where a risk has increased, explain the ways in which the risk could affect the business - "for instance, a cyber attack, loss of sensitive data leading to a lack of customer confidence, a failure of IT systems leading to a failure to operate certain elements of the business, etc." The mitigation description should explain how mitigation has addressed the increased risk profile.

5.2 Guidance from the Securities and Exchange Commission (SEC)

In the USA, there is existing guidance specifically dealing with disclosures around cybersecurity, dating back to 2011.

The Securities and Exchange Commission (SEC) Division of Corporate Finance has issued further interpretive guidance taking effect from 26 February 2018, reminding registrants of their existing responsibilities – including insider trading prohibitions – 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.

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;
- the importance of maintaining comprehensive policies and procedures related to cyber security risks and incidents;
- 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;
  - disclosure of known or threatened cyber incidents to place the risk in context – this encourages discussion of specific real events rather than theoretical events; and
  - 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

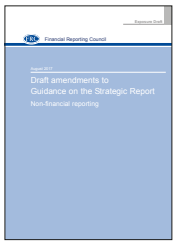
This section pulls together additional resources that may be useful as a deeper dive on governance topics of interest, or which we believe can add insight on cyber risk and the impacts that can be associated with it.

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

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

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

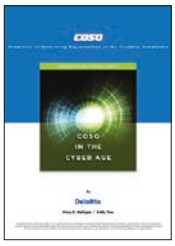


"FRC's Draft amendments to Guidance on the Strategic Report: Non-financial reporting"

External resources – USA

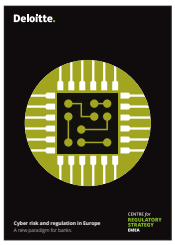
SEC Interpretive Guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents, applicable February 26, 2018.

AICPA Cybersecurity Resource Centre



COSO in the Cyber age

Recommended Deloitte publications



Cyber risk and regulation in Europe: *a new paradigm for banks* explains why banks in Europe should expect a growing level of scrutiny from authorities in how they deal with cyber risk, and greater pressure to demonstrate that they are addressing emerging regulatory concerns in a timely way. Taking steps now to get ahead of the game will be crucial.

Deal breaker: *cyber risk in life sciences M&A* explores how to address cyber risk in life sciences M&A. Life sciences is already one of the most at risk industries from cyber-crime. Given that the industry is also one of the most active in M&A – a unique time when the most sensitive information assets on both sides of a transaction may be more exposed – and you have the perfect storm for cyber-crime.

Demystifying cyber insurance coverage: *Clearing obstacles in a problematic but promising growth market* explores why companies have not more readily signed up for cyber insurance, what roadblocks exist and how the insurance industry can help to clear them.

Why consumer products CMOs should care about cyber risk: *how technology-fueled marketing strategies create vulnerabilities* explores the top cybersecurity threats consumer products CMOs must be aware of and learning around the importance of collaboration between CMOs and their cyber counterparts.

Safeguarding the Internet of Things describes the Information Value Loop, a framework for understanding how organisations create value from information and why secure, vigilant, and resilient systems are essential at each stage of the value loop.

Cyber risk in consumer business discusses the six main cyber risk challenges consumer businesses face today, from customer trust to intellectual property.

Appendix 1: 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 our 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: • 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? *Note: Most FTSE 100 companies in our survey presented cyber risk within operational risks category.*	
4.	Have you disclosed changes to the principal risk(s) associated with cyber since the previous year: • Change in likelihood • Change in potential impact • Change in potential timing *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.*	
5.	Have you disclosed specific types of cyber crime that you have experienced or expect to be exposed to: • 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?	

	Ideas	Y/N
8.	Have you clearly disclosed the potential impact if identified cyber risks were to crystallise: • 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	
	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? *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.*	
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?	

	Ideas	Y/N
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? *Note: Better FTSE 100 annual reports also mention cyber security training provided to the Board.*	
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?	

Appendix 2: Examples of cyber risk disclosure

We have gathered in this appendix a number of illustrative examples of cyber risk disclosure from our survey of the FTSE 100 annual reports.

Example 1

This example from Prudential's annual report provides detail and specifics about the type of cyber crime the business faces.

> As a result of Prudential's increasing market profile, the growing interest by customers to interact with their insurance provider and asset manager through the internet and social media, improved brand awareness and the classification of Prudential as a G-SII, there is an increased likelihood of Prudential being considered a target by cyber criminals. To date, Prudential has not identified a failure or breach which has had a material impact in relation to its legacy and other IT systems and processes. However, it has been, and likely will continue to be, subject to potential damage from computer viruses, attempts at unauthorised access and cyber-security attacks such as 'denial of service' attacks (which, for example, can cause temporary disruption to websites and IT networks), phishing and disruptive software campaigns.

Example 2

Smiths Group provides a good example of describing the potential impact of the risk of a cyber security breach. This also acknowledges the attractiveness of the group's data to cyber criminals.

RISK AND POTENTIAL IMPACT		KEY MITIGATING CONTROLS
PRODUCT QUALITY ISSUE – RECALL / LITIGATION / CATASTROPHIC EVENT RISK APPETITE Current | Target POTENTIAL IMPACT Medium TREND Decreased VELOCITY High	In the ordinary course of business we are subject to litigation such as product liability claims and lawsuits, including potential class actions, alleging that our products have resulted or could result in an unsafe condition or injury. The mission-critical nature of many of our solutions makes the potential consequences of failure worse than would otherwise be the case. Potential impact • Manufacturing flaws, component failures and/or design defects could require us to recall products, many of which are used in critical applications where the consequences of a failure could be extremely serious and, in some cases, potentially catastrophic • The Group, in particular Smiths Detection and Smiths Medical, may potentially be exposed to losses in the event of a cyber security breach relating to the Group's products. These include not only customers' losses, but also those of a potentially large class of third parties • Our businesses are active in markets and product areas that are known to be of interest to cyber criminals	• We have insurance cover for product liability. • The US SAFETY Act provides legislative protection for certain Smiths Detection products in the US; and we support efforts to implement similar legislation in other markets (eg ongoing 'third party limitation' lobbying seeks mirror legislation in the EU) • Quality assurance processes embedded in manufacturing locations for critical equipment, supporting compliance with industry regulations (eg FAA, FDA, API, etc.) • Material litigation is managed under the oversight of the Group General Counsel • Our Group-wide Quality Council drives standard definitions, identifies and shares best practice, and reduces the cost of poor quality • Risk analysis and mitigation processes relating to product cyber resilience are embedded in the product lifecycle process. Proactive steps are taken to ensure product cyber-related risks are continually monitored and managed P56, P180

Example 3

Sage includes cyber risk in its viability statement, including a description of two separate potential information security scenarios.

Viability statement

The viability period

The Directors reviewed the period used for the assessment and determined that a three-year period remained suitable. This period aligns our viability statement with our planning time horizon for our three-year strategic plan and is appropriate given the nature and investment cycle of a technology business. Cash flows over this period have a relatively high degree of predictability, particularly as business moves to the subscription model. Projections beyond this period become less reliable given the inherent uncertainty of technology and market developments.

Assessing viability

The strategy and associated principal risks, which the Board and the Audit and Risk Committee review at least annually, are a foundation for the Group's strategic plan. The plan makes certain assumptions about the uptake of subscription services, the ability to refinance debt as it falls due and the acceptable performance of the core revenue streams and market segments.

The plan was stress tested using sensitivity analysis. To achieve this, management reviewed the principal risks and considered which might threaten the Group's viability. It was determined that none of the individual risks would in isolation compromise the Group's viability, and so a number of different severe but plausible scenarios were considered where principal risks arose in combination.

The scenarios identified and the combination of principal risks involved were as follows.

#	Description of scenario	Principal risks involved
1	An information security incident relating to Sage internal or colleague information, leading to data: – being lost or leaked outside the Group; and/or – becoming corrupted or contaminated; and/or – becoming inaccessible.	– Sage brand – Third party reliance – Supporting control environment – Information management and protection (including cyber) – Legal and regulatory framework
2	An information security incident relating to customers, leading to data: – being lost or leaked outside the Group; and/or – becoming corrupted or contaminated; and/or – becoming inaccessible for the customers.	– Sage brand – Partners and alliances – Third party reliance – Information management and protection (including cyber) – Legal and regulatory framework
3	Sage, or a third party acting on Sage's behalf, fails to comply with legal obligations, leading to: – allegations of bribery or corruption; and/or – allegations of modern slavery; and/or – breach of sanctions.	– Sage brand – Partners and alliances – Third party reliance – Legal and regulatory framework

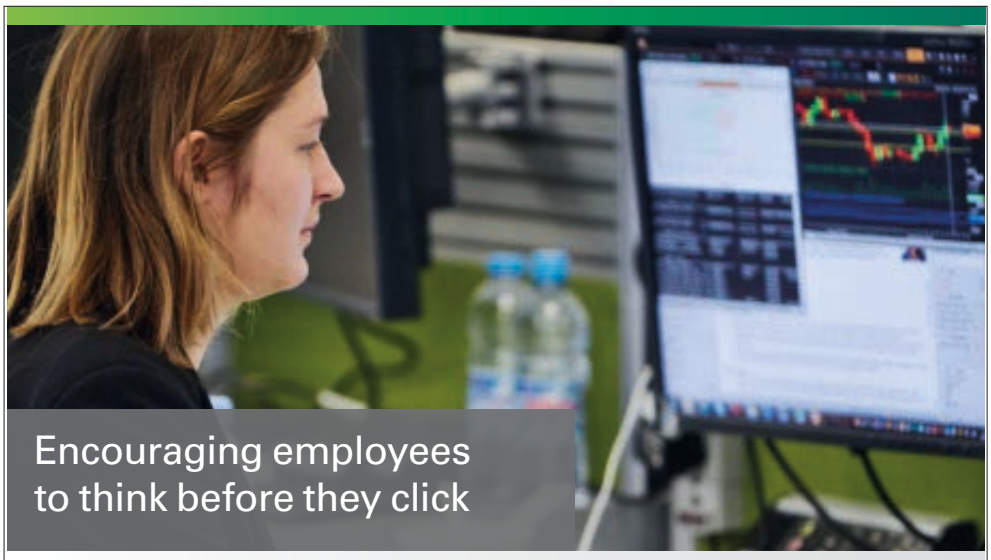
Example 4

Centrica's disclosure on the topic of employee threat, acknowledging the risk posed by disaffected employees.

Description		Potential impacts	Mitigation
12	**Information systems and security** Effectiveness, availability, integrity and security of IT systems and data essential for Centrica's operations. **Governance oversight** Board, Audit Committee and Safety, Health, Environment, Security and Ethics Committee **Risk climate** **Priority** Safety, compliance and conduct	Our substantial customer base and strategic requirement to be at the forefront of technology development, means that it is critical our technology is robust, our systems are secure and our data protected. Sensitive data faces the threat of misappropriation from hackers, viruses and other sources, including disaffected employees.	• Our information security strategy seeks to integrate information systems, personnel and physical aspects in order to prevent, detect and investigate threats and incidents. • We engage with key technology partners and suppliers, to ensure potentially vulnerable systems are identified. • We regularly evaluate the adequacy of our infrastructure and IT security controls, undertake employee awareness and training, and test our contingency and recovery processes. • We test our cyber security crisis management and business continuity plans recognising the evolving nature and pace of the threat landscape. • The appointment of a new Group Chief Information Officer during 2016 has provided additional focus on ensuring that all information systems and security risks are managed appropriately.

Example 5

BP provides a good disclosure regarding employee risk and some of their approaches to managing it.



Encouraging employees to think before they click

We rank cybersecurity as one of our highest priority risks. We deal with attempted cyber attacks on our business every day. Employees are our first line of defence against these attacks and we promote secure behaviours to help mitigate this growing risk. We focus on practical rules that we promote through films, e-learning and sessions delivered by senior managers and our digital security team.

One of our rules addresses 'phishing', which is the attempt to trick people into revealing sensitive information and can involve installing malicious software to steal information without their knowledge. So we remind staff to 'think before you click' and be vigilant for phishing emails, calls and other suspicious requests for information and to report any such attempts to our digital security operations centre.

We conduct 'ethical phishing' tests to educate our employees in this area. The number of employees who click on the links in the test emails has fallen by more than 70% since 2012. Over the same time, there has been a significant increase in the number of employees reporting the phishing tests. The programme is driving real change in awareness, but we remain vigilant as the threat continues to evolve.

Example 6

RELX explains that it relies on and provides data to third parties and how it mitigates the risk, including through actively monitoring the application of RELX policies by third party providers.

OPERATIONAL RISKS

Risk	Description and impact	Mitigation
Technology failure	Our businesses are dependent on electronic platforms and networks, primarily the internet, for delivery of our products and services. These could be adversely affected if our electronic delivery platforms or networks experience a significant failure, interruption or security breach.	We have established procedures for the protection of our technology assets. These include the development of business continuity plans, including IT disaster recovery plans and back-up delivery systems, to reduce business disruption in the event of a major technology failure.
Cyber security	Our businesses maintain online databases and information, including public records and other personal information. As part of maintaining this information and delivering our products and services we rely on, and provide data to, third party service providers. These databases and information are susceptible to cyber attacks where external parties seek unauthorised access to our, or our users', data. Our cyber security measures, and the measures used by our third party service providers, may not detect or prevent all attempts to compromise our systems, which may jeopardise the security of the data we maintain or may disrupt our systems. Failures of our cyber security measures could result in unauthorised access to our systems, misappropriation of our or our users' data, deletion or modification of stored information or other interruption to our business operations. As techniques used to obtain unauthorised access to or to sabotage systems change frequently, and may not be known until launched against us or our third party service providers, we may be unable to anticipate, or implement adequate measures to protect against these attacks. Compromises of our or our third party service providers' systems, or failure to comply with applicable legislation or regulatory or contractual requirements could adversely affect our financial performance, damage our reputation and expose us to risk of loss, litigation and increased regulation.	We have established data privacy and security programmes with the aim of ensuring that data is protected and that we comply with relevant legislative, regulatory and contractual requirements. We have governance mechanisms in place to design and monitor common policies and standards across our businesses. We invest in appropriate administrative, technical, and physical controls which are applied across the enterprise in a risk based security programme which operates at the infrastructure, application and user levels. These controls include, but are not limited to, infrastructure vulnerability management, application scanning and penetration testing, network segmentation, and logging and monitoring. Our administrative controls include training and communication initiatives to establish awareness of risks at all levels of our businesses, and appropriate incident response plans to respond to threats and attacks. We run programmes monitoring the application of our data privacy and security policies by third party service providers. We use independent internal and third party auditors to test, evaluate, and help enhance our procedures and controls. We have established procedures for incorporating the requirements of relevant laws and regulations into our overall security programme, including into our policies and procedures. Our compliance with these is also regularly reviewed and tested.

Example 7

Paddy Power case study regarding how the board, risk committee and audit committee addressed technology-related risks, including cyber risk. It shows that the matters considered at committee level have been pulled together into a comprehensive response at board level.

Case study: Consideration of Technology-related risks, including cyber-risk

Cyber-threats are a feature of operating e-commerce businesses and the Board is acutely aware of the risk. Accordingly, the Board, the Risk Committee and the Audit Committee spent time during the year considering the risk and how we manage it. This included briefings from the Chief Technology Officer and the Director of Technology Security. Management of this risk includes:

- a team of over 50 in-house IT security professionals globally;
- a dedicated Cyber and Threat Management team;
- a 24/7 sweep of the network perimeter to look for weakness;
- regular security testing of all products and services;
- an in-house 'ethical hacking' team that tests our sites and products in the same way as hackers would;
- defensive measures, procedures and teams to protect from malicious distributed denial of service ("DDOS") attacks;
- processes in place to ensure security is built in to product development;
- sharing of proactive threat intelligence as part of industry reviews and discussions;
- a formal Technology Risk Management function to ensure that risks are being appropriately managed; and
- significant annual investment in people, process and technology to stay ahead of threats.

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 details 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

Dominic Cockram
Tel: +44 (0) 20 7303 2288
Email: dcockram@deloitte.co.uk

Peter Gooch
Tel: +44 (0) 20 7303 0972
Email: pgooch@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: csheriff@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.

Designed and produced by The Creative Studio at Deloitte, London. J15008