BENCHMARKING REPORT

Assurance with Vision

Cyber Security Risks

Background

There are very few aspects of our lives that are not reliant on technology and this is never more true than in our work environment. Our increasing business reliance on 3rd party providers and hugely complex supply chains means that, for a cyber criminal, there are endless opportunities to access sensitive information and data to maximise profits and create havoc. Estimates suggest that there are as many as 2000 cyber attacks a week internationally, most recently TalkTalk and the 4m customer accounts that have been put at risk following a "sustained" attack on the company's website and the subsequent 'blackmail'.

This raft of cyber attacks has the potential for multi-million pound financial losses, not to mention denial of service, disruption and substantial reputation damage to organisations.

Every organisation has a duty to ensure that its IT systems are safe and secure, but increasingly, this is not just about preventing access to the systems. In 2012, FBI Director Robert Mueller noted that *"there are only two types of organisations; those that have been hacked and those that will be"*.

360 ASSURANCE

360 Assurance has a clear vision for the delivery of audit and assurance solutions. Our approach is one of Partnership and Collaboration. We work in partnership with you to provide a cost effective, quality driven service that helps you deliver your key priorities.

In This Report

© 360 Assurance, 2015. All rights reserved.

Organisations are now directing resources not just in the prevention of access, but to ensuring that arrangements are in place to detect suspicious activity within the systems. Hackers may spend weeks 'sniffing' around a website, collecting information and data, and testing the weak spots, before launching the final attack. Organisations are getting better at identifying when this activity is taking place by monitoring access patterns to information from seemingly genuine sources, and this is starting to prove valuable in pre-empting attacks, identifying areas of weakness and thus limiting potential damage.

Many cyber attacks are automated and target commonly known weak spots in systems that organisations have just not 'patched up'. Organisations need to implement good, and sometimes basic, technical controls but also ensure that this sits alongside strong user awareness of potential threats. It is also imperative that organisations recognise that issues will not only be coming from external sources and that employees can pose a threat, either intentionally or unintentionally.

The threat to cyber security is not an issue that will go away. It will only increase in frequency and the sophistication of the attacks, and all organisations need to recognise the potential impact this may have on their business activities and make plans accordingly.

Methodology

We reviewed recent advice and guidance on cyber security threats and best practice, as well as reflecting on recent media coverage, to develop our benchmarking survey on cyber security risks. We issued our survey in August 2015 to Governing Body members across the 18 CCGs in our client base. Both executive and non-executive members of Governing Bodies responded with a response rate of over 50%. Not all questions were answered by respondents. Percentages of responses reported in this benchmarking report take account of this and reflect the total number of responses received per question. Items in *italics* included in this benchmarking report are explained in the Glossary of Terms at the end of the report.

Why do health organisations need to take cyber security risks seriously?

Cyber security threats can result in:

- *Theft of patient and employee personal data which can be sold to advertising agencies or criminal organisations.*
- *'Denial of service' attacks and other technical breaches which could impact on IT systems and the ability of an organisation to ensure business continuity, with the ultimate impact being on patient safety and experience.*
- *Damage to an organisation's reputation and financial loss or fines.*

Although traditionally, organisations have shied away from 'airing their dirty linen' in public, there is an emerging recognition that there is a strength in numbers and not re-inventing the wheel when it comes to defending your organisation. As such the sharing of information around cyber attacks and cyber security is becoming increasingly common. In May 2015, the Health and Social Care Information Centre (*HSCIC*) issued guidance on reporting, managing and investigating Information Governance and Cyber Security Incidents. All Cyber Serious Incidents Requiring Investigation (*SIRI*) should now be reported to the Department of Health and *HSCIC*, with key lessons learned from reporting of Cyber SIRIs being reported back through the Senior Information Risk Owner (*SIRO)* network.

January 2016 will also see the launch of a new service, '*CareCERT*', (Care Computing Emergency Response Team), managed by the *HSCIC*, to provide expert advice and guidance on cyber security threats and best practice to health and social care.

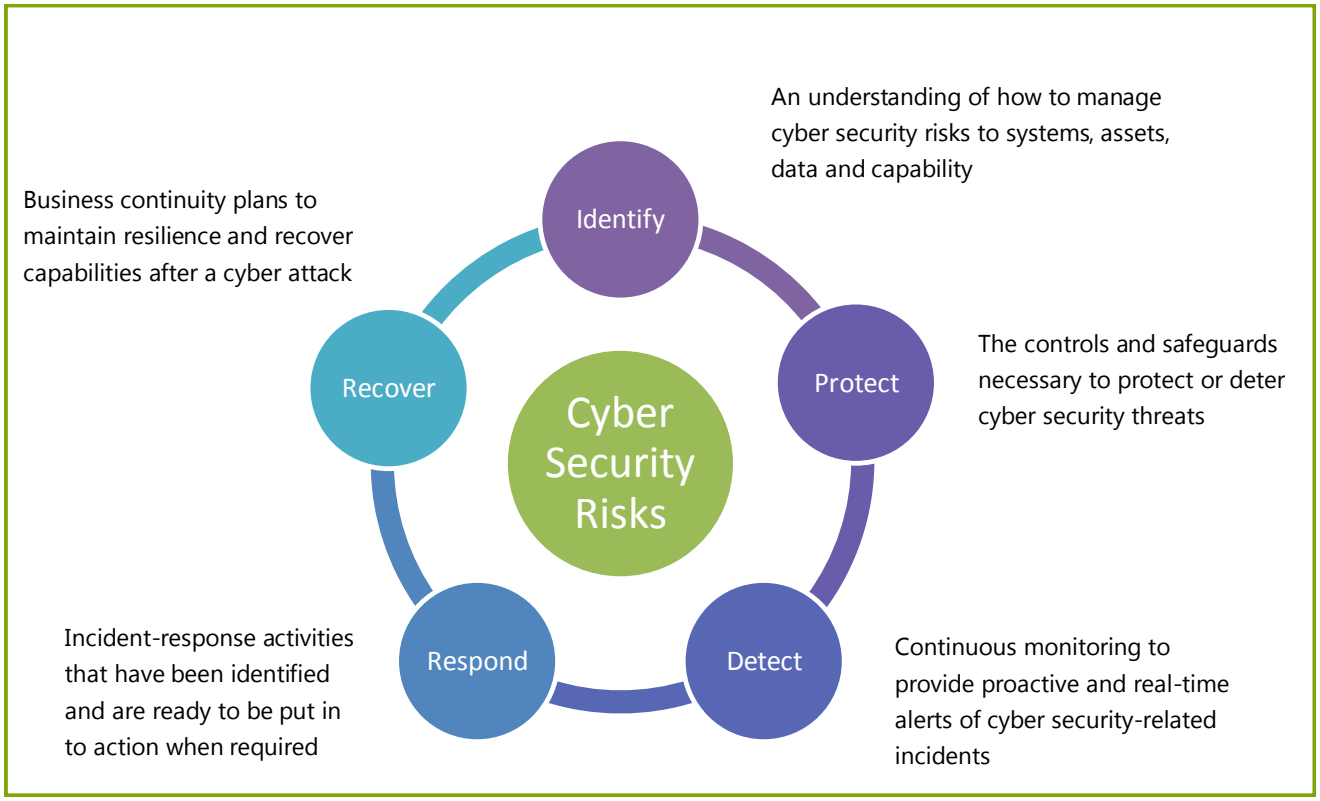
Executive Summary

Throughout this report, we have identified the key messages for organisations when considering how to respond to cyber security risks. Whilst the results are based on a survey of CCG Governing Body members, it is clear from information appearing nationally that these results are in line with concerns across the NHS.

The key theme emerging from the survey is the absence of a comprehensive awareness amongst Governing Body members about cyber security, the extent to which cyber security presents a real risk to an organisation and how organisations are managing the risk. Whilst it is reasonable for non-executive members to be less familiar with the detailed, operational arrangements that an organisation has put in place to manage cyber security risks, such as policies and procedures and training being provided, a key function of the Governing Body is the oversight of risks facing their organisation and obtaining assurance that risks are being managed effectively. To discharge this duty in relation to cyber security will require an increased level of training and development, but also an expansion in the range of assurances received.

Survey results indicate that organisations have not necessarily recognised cyber security risks on either their assurance framework or organisational risk register which means that it is still an area that organisations have yet to get to grips with. It is clear that organisations need to move away from the view that cyber security is just a technical issue and to recognise that, ultimately, cyber security risks can have an impact on patient care and business continuity and needs to be managed accordingly. The recognition of such risks is particularly pertinent for CCGs, given that the majority have outsourced *IT network security* to a third party provider with Governing Bodies not necessarily aware of the assurances that are being received around the effective management of these risks. CCGs must be aware that despite outsourcing services, they retain responsibility for their data, and any failures of 3rd parties handling their data and information.

The Institute of Internal Auditors has identified five core functions of effective cyber security, based on the Cybersecurity Framework drafted by the US Commerce Department's National Institute of Standards and Technology. These provide a useful framework for organisations in thinking about cyber security risks (diagram below).



The Health and Social Care Information Centre's *CareCERT* service, to be launched in January 2016, will provide incident response expertise, will broadcast cyber threats and actions to take and be a central source of security intelligence.

The *HSCIC* Director of Operations and Assurance has said that:

> "***CareCERT* will be another tool to help organisations to meet the high standards of information security which is rightly expected by patients, clinicians and the general public.**"

Key Messages

Governing Body members and staff need to have an appropriate knowledge and understanding of cyber security risks that is relevant to their role and responsibilities.

Organisations may be satisfying basic mandatory training requirements regarding information governance but need to review training needs relating to cyber security risks.

Organisations need to increase awareness of the role of the SIRO.

Knowledge of Cyber Security Risks

Those involved in managing cyber security risks and all users of IT systems need to have appropriate knowledge and understanding of cyber security risks and how they are being managed within their organisations. Risks arising from cyber security threats are relatively new but are rapidly becoming more sophisticated as opportunities for attack increase. This added to relatively low levels of awareness of cyber security, mean that many organisations do not have experience in understanding or dealing with the risks presented, or the consequences.

Within the survey, 48% of respondents reported that they have no existing knowledge of cyber security, with 84% not having received any training on cyber security in the last 12 months. This included 20 of the 22 executive officers who responded to the survey. This is in contrast to the 82% of respondents who had received training on information governance and the 95% who noted a clear understanding of the Information Governance Toolkit that NHS organisations are required to complete annually.

In any organisation, the Senior Information Risk Owner (*SIRO*) has a pivotal role in the management of information risk. 12% of respondents did not know who the SIRO is within their organisations .

Just under half of respondents were not confident that their Governing Body understands cyber security risks. This view was expressed by both executive and non-executive members of Governing Bodies.

Only 11% of respondents reported that cyber security risks are being actively managed by the Governing Body/Board throughout the year.

Key Messages

Cyber security should be approached as an organisation wide risk issue, not just an IT one, and one which is ultimately the responsibility of the Governing Body.

We asked respondents to rank the likelihood of cyber security threats occurring. Most identified accidental loss or damage as being the most likely threat to occur, followed by *phishing* emails and *criminal fraud threats*. *Hacktivists* and those who attack for political or ideological motives were considered the least likely to occur.

When asked about the consequences to their organisation, the highest number of respondents (48%) ranked reputational damage as being the greatest risk, followed by business continuity being compromised (23%), legal or contractual sanctions (16%) and then financial costs (12%).

The extent to which organisations have experienced cyber security threats or incidents is unclear. Whilst only 8% of respondents reported that their organisations had experienced a cyber security threat or incident, 51% of respondents had no knowledge of whether their organisation had experienced an incident or not. Where organisations had a cyber security threat or incident, only one respondent identified that it had been reported to the Governing Body, whilst four respondents identified reporting to a relevant committee or forum.

The Government, in conjunction with industry, has developed the *Cyber Essentials Scheme*. The Scheme provides a clear statement of the basic controls that all organisations should implement to mitigate the risk from common internet based threats. It also provides, through its assurance framework, a mechanism for organisations to demonstrate that they are implementing these basic cyber security controls and obtain accreditation for this.

Key Messages

Organisations could consider accreditation under the *Cyber Essentials Scheme*.

88% of respondents did not know if their organisations had received external accreditation against the *Cyber Essentials Scheme* and only 1% of respondents knew how to gain accreditation and what it requires.

60% of respondents reported that cyber security risk is either a technical topic not warranting Governing Body attention or that it is not currently regular business for the Governing Body.

Cyber security threats can come from many sources, including:

- *Criminal fraud threats*
- '*Social engineering*', or direct contact with staff to trick them in to releasing information
- Internal, disgruntled employees
- Accidental loss or damage
- *Technical security* issues
- *Phishing* emails
- *Hacktivists* and those who attack for political or ideological motives.

Key Messages

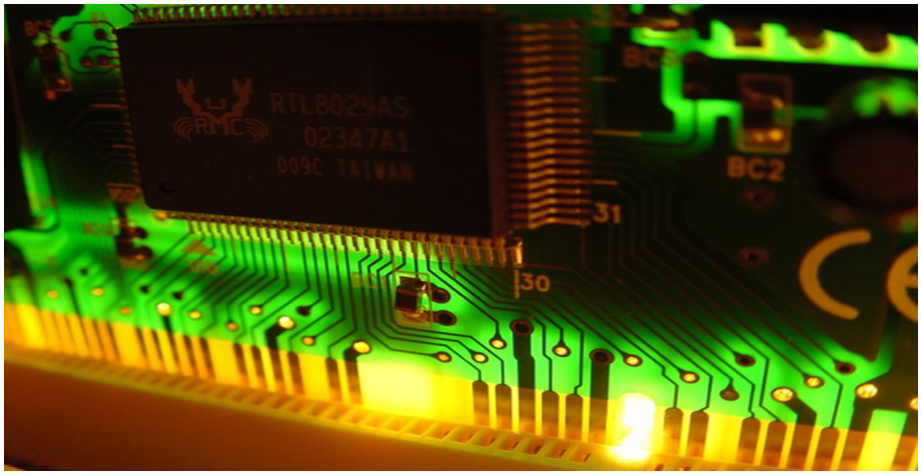
The Governing Body should understand the cyber security risks associated with 3rd party providers and obtain assurances that security and privacy requirements are clearly understood when contracts are negotiated.

Where organisations are sharing information with each other, the Governing Body should satisfy itself that there are robust data and risk sharing protocols in place to address cyber security.

Organisations should not only be concerned with the risk of cyber security threats to themselves but should also consider the effects such threats may have on those they contract with. The complexity of supply and information chains means that there is an increasing possibility of consequences for an organisation through their association with other businesses. Whilst 46% of respondents thought that requirements for information governance and cyber security are included in contracts with providers and associates, the majority of respondents indicated that they did not know how these requirements were managed. At the same time, 67% of respondents were not aware if their organisation had been informed of any cyber security risks or security breaches within the provider organisations or institutions with whom they contract.

This issue will inevitably be extended with the transformation and integration agenda. Data and information is flowing not only between NHS organisations but increasingly with organisations that work with and support the NHS and as such, the level of exposure is multiplied.

Organisations must ensure that they have proper assurances around the security arrangements within all organisations with whom they share data and information.



Oversight of Cyber Security Risks

Key Messages

Organisations should already have established risk management arrangements through which cyber security risks can be considered, understood and managed.

The use of technology has brought huge benefits to organisations, transforming how they can access and organise information and communicate with others. At the same time, it has given rise to new levels of risks that are constantly evolving and which need to be understood and managed.

Governance frameworks must support the management of information risks across the organisation, with ultimate responsibility for risk ownership residing at Governing Body level. Organisations will already have established risk management arrangements which should help in ensuring that cyber security risks can be considered, understood and managed effectively in the same way as legal, regulatory, financial or operational risks.

Our survey results suggest, however, that organisations may not yet have fully considered the potential cyber security risks associated with the use of technology as relatively few organisations appear to have recognised this area as a risk.

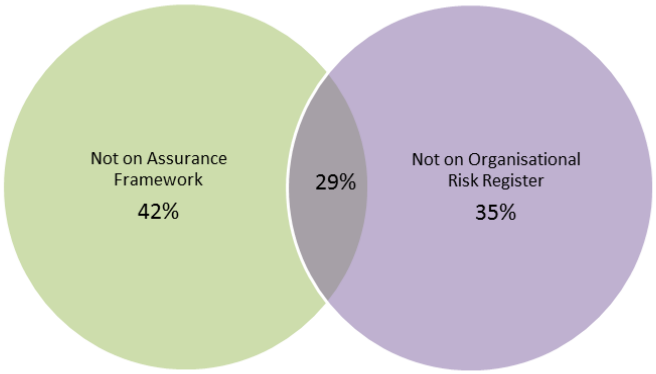
Key Messages

Given the potential for reputational damage, impact on business continuity and possible financial loss, organisations should recognise cyber security threats on either their Assurance Framework or Organisational Risk Register and regularly review their rating of cyber security threats.

Following notification of a cyber security incident, organisations should be asking themselves "could this happen here?"

Groups responsible for the oversight of risks should regularly engage with 3rd party providers.

Has your organisation recognised cyber security as a risk on its Assurance Framework or Organisational Risk Register?



When asked where within the organisation cyber risks were managed, 34% of respondents did not know, which is why it was unsurprising that, overall, nearly a third of respondents reported that cyber security has not been recognised on either their organisation's assurance framework or risk register.

Where cyber security has been recognised as a risk, most respondents were not aware of the risk rating (i.e. High, Medium, Low). Where this was known, none had rated it as high. The ratings used do not appear to reflect the potential impact of cyber security risks given that respondents ranked reputational damage, business continuity being compromised and financial costs as the greatest risks to their organisations.

In relation to the oversight and management of cyber security risks, the *SIRO* plays a key role, being the person with overall responsibility for an organisation's information risk policy. Only 33% of respondents reported that the *SIRO* sits on the committee or forum with the main responsibility for cyber security risks. 39% of respondents did not know who sits on the committee or forum.

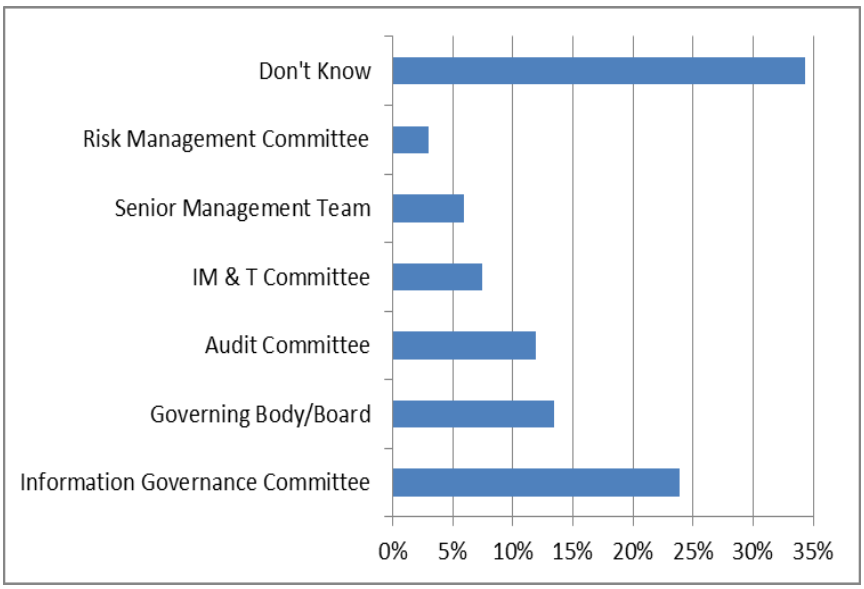
Key Messages

Cyber security should be considered at Governing Body level and assurances be obtained that risks are being managed effectively.

The SIRO should be a member of the committee or forum with the main responsibility for oversight of cyber security risks.

We did note, however, that where there was an awareness of the group responsible for oversight, the officers noted as being part of the group were appropriately senior within the organisation. It was also noted that operational officers, such as the IT Manager were included, as were representatives from 3rd party providers, which offers the opportunity for a level of challenge regarding arrangements.

Which committee / forum has the main responsibility for oversight of cyber security risks?



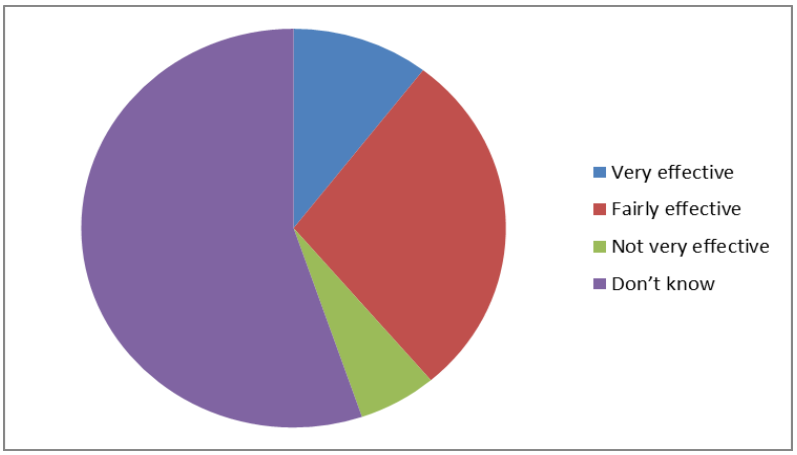
When asked about how effective the committee or forum is in its oversight of cyber security risks, over half of respondents (55%) did not know. A further 5% did not think it was effective.

Only 22% of respondents reported that this committee or forum and its members are regularly involved in reporting cyber security risks across the organisation.

Key Messages

Organisations should review where responsibility for oversight of cyber security risks has been assigned within their governance structures to ensure it is appropriate and provides for escalation of issues to the Governing Body when required.

How effective do you think the committee / forum is in its oversight of the organisation's cyber security risks?



Questions must be asked, therefore, about the extent to which Governing Body members are assured that cyber security risks are being managed effectively within their organisations, either because they do not know where those risks are being managed and reported or they consider that the committee or forum is not effective in its management of them.

Clearly, in some organisations it may be necessary to review where responsibility for cyber security risks has been assigned to ensure that this continues to be appropriate.

Although it can delegate responsibility to a sub-committee, as with all risks, ultimately, the Governing Body is responsible and will need to receive assurances around effective management.

Key Messages

Organisations should know what their *information assets* are.

Organisations should assign responsibility to *information asset owners* and ensure there is a direct reporting line to the *SIRO* and the Governing Body.

Managing Cyber Security Risks

Identifying Information Assets

An *information asset* is typically a piece of information, for example, a patient or employee record or financial report which is valuable to an organisation, but it might also be operating systems and computer applications. An organisation needs to know what constitutes its most precious information and data and why they are important. By doing this an organisation can make informed decisions as to the extent that it needs to implement protection and prioritise its resources and controls. It needs to know where this data and information is kept and how access to it is controlled and the impact of the loss, theft or corruption of these information assets on the organisation's ability to deliver on it's objectives and business imperatives.

The survey has suggested a lack of knowledge about the extent to which officers within the organisation identify, understand and manage information assets. 52% of respondents did not know if their organisation periodically carries out a review to identify potentially sensitive or valuable information and of these, 14% were executive officers. Almost half of respondents did not know if staff have been made aware of what constitutes an *information asset*, with 55% of respondents not knowing if *information asset owners* have been identified in their organisation.

When asked about how confident respondents were that their organisation had identified all key *information assets* and assessed their vulnerability to attack, 39% of respondents reported that they were not very confident.

Key Messages

Business Continuity or Resilience Plans should incorporate cyber security risks.

The Governing Body should receive assurance that the Business Continuity or Resilience Plan has been tested. This should relate to both internal recovery and continuity plans and those of 3rd party service providers.

Staff Training and Awareness

There should be clear information risk management policies covering acceptable and secure use of an organisation's systems, which include a formal training programme for employees and officers, incorporating cyber security risks.

The Government has launched the '10 steps to cyber security' and this summarises the importance of having information risk management policies and ensuring user education and awareness.

(https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)

Compliance with policies and procedures should be regularly reviewed and monitored with arrangements for responding to threats, should they arise, being established and periodically tested.

60% of respondents did not think or were unsure whether their organisation's Business Continuity or Resilience Plan incorporated cyber security risks. At the same time, 54% of respondents did not know if their organisation's Business Continuity or Resilience Plan had been tested.

Key Messages

The training programme for IGM&T policies and procedures should be reviewed and methods to test compliance should be introduced.

Proper process must be established to ensure that policies and procedures are regularly updated.

When it comes to the threat posed unintentionally from employees there is a need to ensure that all staff have access to proper training and information in relation to information governance and their individual responsibilities, whether this is bringing external devices into their organisations and 'plugging' them into the systems, or whether it is responding to potentially damaging phishing emails.

We asked a number of questions in relation to the Information Governance and Management of Technology policies that were available to staff.

- 50% of respondents overall reported that either their organisation has no policy on *Bring Your Own Devices to work (BYOD)* or they were unsure whether there is such a policy.
- Approximately a third did not know if there was a policy on *removable media*, home and mobile working or use of social media.
- 35% of respondents did not know if staff have received information on IGM&T policies and procedures in the last year.

Key Messages

The Governing Body should receive assurance that cyber security threats are being appropriately managed through the service level agreements in place for *technical security* with external third party providers.

- 57% did not think, or were unsure whether staff have received appropriate training on cyber security risks at induction.
- 71% did not know, or were unsure, if cyber security is covered in refresher training.
- 52% did not know if their organisation has tested its compliance with its IGM&T policies and procedures.
- 41% of respondents did not think, or were unsure whether, processes are in place to review their organisations' risks and preparedness should a breach occur.

Technical Support

Most CCGs (nearly 60%) have outsourced *IT security* to external providers, for example, Health Informatics Services. This is usually recorded within Service Level Agreements and Specifications which need to be reviewed and signed off by both organisations although legal responsibility remains with CCGs as the statutory bodies.

Service Level Agreements should be subject to ongoing monitoring and oversight, however, 62%, of respondents were unsure whether their organisation receives assurances from the third party IT provider on a periodic basis about managing cyber security risks. This again goes to the key finding of this survey, the extent to which members of the Governing Body are informed, or otherwise, of issues and assurances relating to cyber security.

Glossary of Terms

Bring Your Own Devices to Work (BYOD) Organisations may be faced with demands from employees and board members wishing to use electronic devices such as smart phones and tablet computers to carry out their jobs. This might mean that individuals' own devices are used to access and store corporate information, as well as their own personal information. It is important that users connecting their own devices to IT systems clearly understand their responsibilities.

Caldicott Guardian A senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. It is mandated that each NHS organisation has a Caldicott Guardian.

CareCERT HSCIC has been commissioned by the Department of Health to develop a Care Computer Emergency Response Team (CareCERT). CareCERT will focus on providing cyber security intelligence and advice to the health and social care system.

Criminal Fraud Threats Theft of personal data which could increase potential exposure to various forms of identity theft.

Cyber crime The use of computer technologies to commit a crime.

Cyber Essentials Scheme This is a Government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. The Cyber Essentials Badge allows an organisation to confirm that it has been accredited and adheres to a Government endorsed standard.

Cyber Incident Anything that could or has compromised information assets within cyberspace.

Cyberspace The independent network of information technology infrastructures. It includes the internet, telecommunication networks, computer systems and embedded processors and controllers in various industries.

Hacktivist Someone who gains unauthorised access to a computer system and carrying out various disruptive actions.

Health & Social Care Information Centre (HSCIC) National provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care. HSCIC is an executive non-departmental public body, sponsored by the Department of Health.

Information Assets Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, records and information that have value to an organisation.

Information Asset Owner An Information Asset Owner is directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

Information Commissioners Office The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

IT Network Security These activities protect the usability, reliability, integrity, and safety of the network and data. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components often include anti-virus and anti-spyware, firewall to block unauthorised access to networks, intrusion prevention systems (IPS) to identify fast-spreading threats and Virtual Private Networks (VPNs) to provide secure remote access.

Phishing Emails Phishing is a fraudulent method of extracting personal and financial information from recipients by sending emails or using instant messaging services that look legitimate enough for users to disclose the information required. In a typical phishing attempt, an email to a person appears to have come from a trustworthy enterprise, thereby tempting the user to disclose personal information such as usernames, passwords, financial details and the like.

Policy for Removable Media Refers to all types of computer storage which are not physically fixed inside a computer and includes (but is not limited to) memory cards, USB pen drives, removable or external hard disk drives and mobile devices (for example, iPod, iPhone, iPad, MP3 player).

Serious Incident Requiring Investigation (SIRI) This is the requirement to disclose certain incidents in accordance with the guidance issued by HSCIC in May 2015. The guidance applies to all organisations providing or supporting health, public health and adult social care in England.

Senior Information Risk Owner (SIRO) An Executive Director or Senior Management Board Member who will take overall responsibility for the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accountable Officer on the content of the Organisation's Statement of Internal Control in relation to information risk.

Social Engineering A non-technical method intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

Technical Security A very common type of security used in organisations which use computers or nearly any type of technology. It deals with detecting loopholes in a security system and finding adequate solutions to address the risk of technical failure or hacking.

User Security Policy To protect IT infrastructure and the information stored, organisations should develop and implement appropriate security policies. An information security policy facilitates the communication of security procedures to users and makes them more aware of potential security threats and associated business risks.

May we take this opportunity to thank all those who took the time to respond to our survey.

Although this report summarises the key issues from the survey, full details of the results of all the questions are available on request.

FOR YOUR NOTES

360 ASSURANCE

Assurance with Vision

Contact Us

Call for more information about our services.

0116 225 6114

Visit us on the web at www.360assurance.co.uk

360 Assurance:
Riverside House
Bridge Park Road
Thurmaston
Leicester
LE4 8BL

360 Assurance:
Stapleford Care Centre
Church Street
Stapleford
Nottingham
NG9 8DB

360 Assurance:
Oak House
Moorhead Way
Bramley
Rotherham
S66 1YY

Key Contacts

Annette Tudor, Deputy Director	0116 225 6124
Andy Mellor, Client Manager and lead for IM&T	0115 883 5315
Claire Page, Client Manager	0115 883 5310
Tiffany Hey, Assistant Client Manager	0115 883 5310