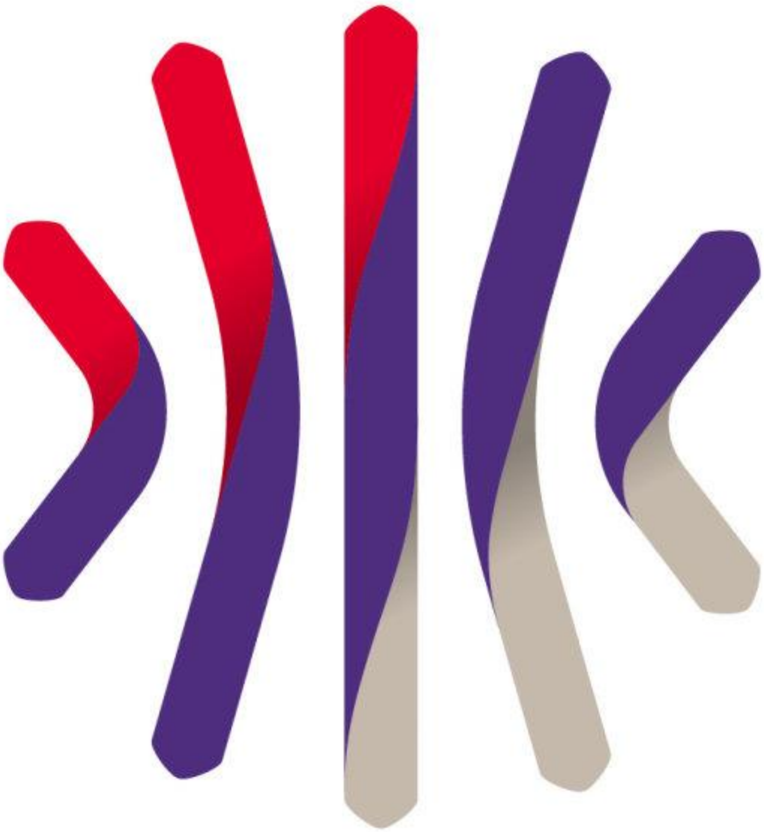
Grant Thornton
An instinct for growth™

Cyber Health Check



NHS Lothian

Report Date: 31 May 2019

James Arthur
Partner, Head of Cyber Consulting
T: +44 2078 652969
E: james.ag.arthur@uk.gt.com

Table of Contents

Executive Summary

Against the UK NCSC 10-Steps to cyber your company are assessed as:

0

HIGH RISK

3

MEDIUM RISK
Key Risks
Removable Media Controls
Home and Mobile Working

8

LOW RISK
Risk Management
Security Configuration
Network Security
Managed User Privilege
User Education and Awareness
Incident Management
Malware Analysis
Monitoring

Your overall risk profile is rated as: LOW

Category	Score	Explanation
Key Risks	45 out of 55	There are a number of key cyber risks in your organisation.
Risk Management	20 out of 20	You have reported that you have the appropriate risk management policies in line with the UK NCSC and good buy-in from senior management.
Security Configuration	20 out of 20	You may benefit from increasing the frequency of your vulnerability scans and assessing your current security configurations.
Network Security	20 out of 20	You have reported that you are following best practice for network security.
Managed User Privilege	20 out of 20	You have reported that you manage user access and privileges in line with current best practice from UK NCSC.
User Education and Awareness	15 out of 15	You have reported you have strong user education and awareness controls with staff regularly trained on the AUP and meaningful action taken in the event of non-compliance with cyber policies.
Incident Management	20 out of 20	You have reported that you are following best practice for cyber incident management.
Malware Analysis	10 out of 10	You have reported that you are following best practice and have effective anti-malware policies and standards implemented across your infrastructure.
Monitoring	25 out of 25	You have reported that you actively monitor systems for threats and compromise in line with UK NCSC guidance.
Removable Media Controls	16 out of 20	You should review current policies and processes against UK NCSC guides and best practice. You should refresh policies and solutions around the control and the use of removable media. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms.
Home and Mobile Working	5 out of 10	Although your corporate ICT devices all use some form of encryption at rest you may benefit from publishing a formal home and mobile working policy.

Introduction

INSTRUCTIONS

I. Grant Thornton UK LLP (or we) have been instructed by NHS Lothian (the Company, or you), to undertake an assessment of the Company's cyber security strengths and weaknesses using our proprietary cyber assessment questionnaire (the Assessment). Our questionnaire is based on UK Government National Cyber Security Centre (NCSC) 10-steps to cyber security guidance.

II. We have also been instructed to prepare this report (our Report), setting out the results of the Assessment and key observations arising from your responses to the Assessment against industry best practice, including an assessment of your cyber security posture (based on your responses) in 11 categories.

III. If further information is produced and brought to our attention after service of our Report, we reserve the right to revise our Report as appropriate. However, we are under no absolute obligation to do so, nor to amend our Report (or any report to you in any form) following its issuing.

IV. Except to the extent set out in our Report, we have relied upon the documents and information provided to us as being accurate and genuine.

LIMITATIONS OF SCOPE

V. For the avoidance of doubt, we do not validate the effectiveness of the Company's information security/cyber controls in undertaking the Assessment. The Assessment is not designed (and therefore should not be relied upon) to provide a comprehensive identification of any information security and cyber threats or other irregularities that may exist.

VI. Any management decisions made by you in connection with this report will remain entirely the responsibility of the Company.

VII. The results of the Assessment are based on the answers provided by the Company during the Assessment and it is the responsibility of the Company to ensure that the responses provided to the questions in the Assessment are accurate.

RESTRICTION ON CIRCULATION

VIII. The report is confidential and should not be used, reproduced or circulated for any other purpose, in whole or in part, without our prior written consent. Such consent will only be given after full consideration of all the circumstances at the time.

IX. No responsibility is accepted to anyone other than the Company.

FORMS OF REPORT

X. For your convenience, our Report may have been made available to recipients in electronic as well as hard copy format. Multiple copies and versions of our Report may therefore exist in different media and in the case of any discrepancy the final signed electronic copy should be regarded as definitive.

Priority Findings

I. We met with you on the 8 May 2019 to obtain your answers to our Cyber Security Health Check questionnaire. We have used your answers to undertake the scoring component of the Assessment, the results of which are summarised below.

II. It is recognised that the company may not have resources immediately available to implement the full range of advice. Therefore, you may benefit from considering prioritising the following areas:

- Although the updating of unsupported operating systems has already been noted as a requirement during our discussion, you may benefit from including this as a prioritised action. Unsupported software/applications can present a huge security risk, as they provide an easy target for both cyber criminals and general computer enthusiasts looking to trial their hacking skills and exploits. It may be beneficial to ensure that all applications and operating systems are updated to a supported version at minimum, while also managing the patching process.

- Cyber Essentials Plus (CE+) is a recognised certification and a great way to baseline security controls. Given the size of the organisation, this may be achieved by breaking down areas of the business into smaller sub-sections and conducting the assessment on these specific areas. Our Vulnerability Scanning Service can be used to provide CE+ certification on the basis of the scans or aid towards the achievement of CE+ if it is likely that you may fail.

- The UK NCSC have produced guidelines on password strength and complexity and should be followed as a minimum standard. Simple passwords can be easily ‘guessed’ and automatic password generating tools used to attempt to access any accounts using insecure passwords. A policy should be in place across the organisation preventing any users from choosing insecure passwords for any systems.

- Allowing the use of removable media may introduce unnecessary risk. If a user can insert their personal USB devices on the corporate network, the chance of introducing malware or virus to the corporate devices increases. You do currently perform virus scans on all inserted devices, however completely removing the ability to use removable media, where it is not required, eradicates the associated threats.

- IT policies are currently in place however one does not exist specifically for mobile working. Information/Data taken outside of the organisation (i.e. a user working on a laptop from home) introduces a number of risks that may not exist inside the usual working environment meaning. Having a specific mobile working policy in place ensures standards are retained both inside the organisation and remotely.

Questionnaire Results: Company Details

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
0.1	How many users does the system being assessed currently have?	29,500		
0.2	What industry is the company in?	NHS		
0.3	Does the Company hold any current cyber security certifications?	Yes Cyber Essentials, obtained last year, currently working towards Cyber Essentials Plus		Best practice is for organisations to adopt a recognised baseline of security controls, such as those defined in Cyber Essentials. This approach does not require any risk analysis, rather it concentrates on applying basic security controls and demonstrating that your organisation takes cyber security seriously. Consider whether the security accreditation you choose takes into account any laws and regulations your organisation must comply with

Key Risks

Risk is a necessary part of business in order to create opportunities and help deliver business objectives. The information contained in this section highlights areas marked as key cyber risks and should be addressed accordingly.

OVERALL RAG STATUS

Scoring:
45/55

Question Breakdown

2 **0** **9**

Questionnaire Results: Key Risks

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
1.1	Can you access any core services (such as email, web content etc.) using only a username and password from the internet? If yes, please list….	No		Best practice is that multi-factor authentication should be strongly considered for all web-facing services wherever possible. Most users are already accustomed to authenticating themselves in their personal lives, as many providers of online services like home banking, social media and email have adopted mobile-based apps to effectively authenticate users when accessing their systems. Not having multifactor authentication in place significantly increases the risk of successful external attacks.
1.2	Are you using any legacy or un-supported software (e.g. Windows NT, Industrial Control Systems (ICS)) for critical business services or data storage? If yes, please list….	Yes Very small number of XP machines, not networked. Small number (8 – 10) machines with windows 2003 working to remove	Use supported software: Use versions of operating systems, web browsers and applications that are vendor (or community) supported.	Most legacy systems are incompatible with newer systems and devices. It's essential that software, no matter how old, integrates well with the tools and applications you require to efficiently run your organisation.
1.3	Are normal users allowed to install software on their corporate devices (e.g. laptops) without the assistance of the ICT department?	No		A large risk exists when allowing normal users to install software on their corporate devices without the assistance of the IT department. This is due to users potentially forgetting to update the correct version of the software. Software companies release new versions to correct or patch security flaws. Keeping on top of downloading or updating the relevant updated software is critical. A hacker may discover and exploit the flaws which allows access into your organisation's network and increases potential for a cyberattack.

Questionnaire Results: Key Risks

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
1.4	Have you ensured that you have changed all default manufacturer credentials (e.g. root passwords) on all of your IT equipment (e.g. routers, databases, firewalls)?	Yes		Hackers use specific malware to scan and search for an organisation's systems/devices still set with default passwords or usernames. Most manufacturers will list on the Internet the default passwords and usernames for their specific devices/systems. If you have installed those systems/devices and not changed the default settings, a hacker will then potentially have access into your network.

Questionnaire Results: Key Risks

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
1.5	Do you allow remote access to your systems for maintenance, remote working or other requirements? If so, how are these protected?	Yes 3rd party access with account enabled for required amount of time	Assess the risks and create a mobile working policy: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed. Protect data at rest: Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.	Remote access provides Managed Services Providers (MSPs) the flexibility to perform a wide range of IT tasks from anywhere. These tasks include everything from IT maintenance and troubleshooting to asset tracking and bandwidth monitoring. Best practice is to ensure that you are satisfied with the level of security on each remote access channel and that any external companies who have remote access to your systems audit the use of this and provide you with a regular report.

Questionnaire Results: Key Risks

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
1.6	Are your IT department applying all manufacturer recommended security patches (for hardware and software) within 14 days of release?	Yes		Opting for an automatic patch management process can enable an organisation to repair existing vulnerabilities in real time which can drastically reduce the risk of cyberattacks. With the automatic clock system, all patches will be updated without any manual process. Eliminating the threat of any patches not being updated reduces open virtual gates for hackers to exploit.
1.7	Are you running active anti-malware/anti-virus software across your entire network and is it configured to automatically scan webpages and files when opened?	Yes		End users on a network may have poor online/Internet habits. These may include downloading an infected piece of software. These habits, if not addressed, will increase the chance of the network becoming compromised. Best practice involves installing anti-malware/anti-virus software across your network which will enable your organisation to have a lower risk browsing system, decreasing the chance of a cyberattack.
1.8	Are you aware of having been the target of a cyber-attack (including insider leaking/stealing data) in the last 2 years?	Yes		It is possible that you may have been a target of a cyberattack over the last two years but are unaware of this. On average it takes an organisation 146 days to identify a cyber breach.
1.9	Have you ever undertaken a penetration test of your network? If so, when was the last one conducted?	Yes Last 6 months		Best practice suggests that penetration testing should be viewed as a method for gaining assurance of an organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities.

Questionnaire Results: Key Risks

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
1.10	Is your password policy in line with UK NCSC guidance?	No Identified AD password does not comply. Currently being updated	Establish policies and standards for user authentication and access control: A corporate password policy should be developed that seeks an effective balance between security and usability as set out in the UK NCSC's password guidance. For some accounts an additional authentication factor (such as a token) may be appropriate.	Education on how to identify a strong password can make a difference in the defence against a cyberattack. Instructing users with password configuration tips and techniques can lower your risk. Further guidance on passwords from the UK NCSC can be found at the following website: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
1.11	Do you have a data backup strategy in place? If so, when was the last time this was tested?	Yes Last 6 months		Data back-up is vital to the continuity plan of any organisation. Data should be backed up in multiple formats e.g. cloud storage and physical storage units as well as held in separate/segregated locations to minimise the impact of any data loss.

Risk Management

Organisations rely on technology, systems and information to support their business goals. It is important that organisations apply a similar level of rigour to assessing the risks to technology, systems and information assets as they would to other risks that might have a material business impact, such as regulatory, financial or operational risks. This can be achieved by embedding an appropriate risk management regime across the organisation, which is actively supported by the Board, senior managers and an empowered governance structure.

🟩 **OVERALL RAG STATUS**

Scoring: 20/20

Question Breakdown

🔴 0

🟡 0

🟢 4

Questionnaire Results: Risk Management

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
2.1	Do you have a formal risk management process in place that includes consideration of cyber/ICT risk?	Yes		The threat landscape is dynamic and risk management processes need to reflect this. Ensure your processes are updated along with your policies.
2.2	Does senior management understand and engage with risk mitigation processes and promote a risk management culture?	Yes		Risk is easier to manage if everyone has a part to play. Best practice is that senior management should promote a risk management culture and inform all staff, whatever their level, that they have a responsibility to adhere to risk mitigation processes.
2.3	Does the board engage with management and review risks that may arise with new technology used in the organisation?	Yes		The technology organisations use is evolving rapidly. More and more organisations are integrating new technology daily. This integration can come with risks that may not have been previously considered. Best practice is that management should consider the implications of adopting new technology in their environment and the potential risk involved.
2.4	Do you have a formal technology/ICT risk management policy? If yes, is this communicated to all staff?	Yes		A risk management policy should be created that is dedicated to the risks associated with the technology and IT specific to your organisation.

Security Configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

OVERALL RAG STATUS

Scoring: 20/20

Question Breakdown

🔴 0

🟡 0

🟢 4

Questionnaire Results: Security Configuration

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
3.1	Is there an up to date inventory of hardware and software maintained in your organisation? How often is this updated?	Yes Every 3 months		Best practice is that an up to date inventory of hardware and software is held. It should be updated whenever equipment/software is added, removed or updated. This will aid a timely response to any potential incident.
3.2	Are automated vulnerability scans conducted regularly? If so, how often?	Yes Every month		If you do not have the resources to operate your own vulnerability scanners, then consider using vulnerability scanning as a service. Fixing vulnerabilities before attackers can identify these and exploit them will help to defend your network.
3.3	Does your firm apply standard security configurations to each ICT asset (e.g. laptop, phone) that is issued or connected to your networks under a Bring Your Own Device (BYOD) policy?	Yes		Mobile Application Management (MAM) is another security configuration that organisations have to consider on either IT assets or Bring Your Own Devices (BYOD). IOS and Android 'off the shelf apps' sometimes have their own layer of security and control, however, don't fall under standard security configurations and policy. Best practice involves making sure that any of your organisation's data saved on the BYOD device is backed up on corporate devices as well. BYOD users can often rely on just the device itself to save data. An organisation should communicate and make sure there are clear boundaries. You should explicitly describe the consequences of policy violations. BYOD requires mutual trust between an organisation and its employees.
3.4	Do you treat potentially higher risk device users (e.g. non-executive board members, temporary staff) any differently from a security perspective? If so, how?	No – use least user privilege	Limit user privileges: Users should be provided with reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role.	Ensuring end users have only the privileges required to perform their role is another step towards securing your network. It is unlikely that a front-of-house assistant will require admin privileges. This helps prevent both malicious and non-malicious (accidental) security incidents.

Network Security

The connections from your networks to the Internet, and other partner networks, expose your systems and technology to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites, and the use of mobile or remote working and cloud services makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

OVERALL RAG STATUS

Scoring:
20/20

Question Breakdown

🔴 0 🟡 0 🟢 4

Questionnaire Results: Network Security

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
4.1	Does your firm control internet traffic entering your network - for example, are there rules for what internet traffic is allowed by protocol and application?	Yes		Disallowing unnecessary Internet traffic helps prevent attacks. If an application, protocol or URL is not relevant to the day to day running of your organisation, consider blocking it/them.
4.2	Are firewalls or other devices used across the boundary when exchanging information from outside the organisation to internal networks?	Yes		Even with correct firewalls in place, best practice is to make sure the rules and signatures they enforce are reviewed regularly as the protection they provide will only be as effective as the last update.
4.3	Are there any connections from the internet/external systems straight into your internal networks that are not checked (e.g. remote dial-in support from manufacturer, legacy Industrial Control Systems (ICS))?	No		If connections aren't checked, the prevention and detection tools that are deployed on the network might be less consistent in the way they are automatically managed. This inconsistency can lead to an increase of potential cyberattacks.
4.4	If you have Wi-Fi services do you have separate networks for guests and corporate users? If yes, do they only allow known devices to connect to the corporate Wi-Fi?	Yes		The extra cost to add a guest can be minimal, since most guest users will check their emails or use social media platforms. As such, there shouldn't be much bandwidth usage. Best practice is that your business network should be kept separate from your guest access. If not, then every time you let a visitor into your Wi-Fi, they could potentially allow a breach into your corporate network.

Managed User Privilege

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

🟩 **OVERALL RAG STATUS**

Scoring:
20/20

Question Breakdown

🔴 **0** 🟡 **0** 🟢 **4**

Questionnaire Results: Managed User Privilege

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
5.1	Do you actively limit the number of users with administrative accounts or other privileged access?	Yes		The administrator account is the most powerful account that is available in the operating system. Best practice is that this account should not be used unless there is a specific need, such as disaster recovery or initial configurations.
5.2	(If there is a security policy) Is there a policy and standard for user authentication and access control?	Yes		In a data breach, access controls are among the first policies investigated. They are a key component in keeping overall data secure.
5.3	Are normal users only given the permissions to access and use the systems, services and information to fulfil their business roles?	Yes		If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as ‘principle of least privilege’.

Questionnaire Results: Managed User Privilege

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
5.4	Is user activity on your systems currently monitored? If yes, please provide a brief description of how?	Yes Use FairWarning. Highlights potentially inappropriate activity		Monitoring solutions typically collect and store security logs from network devices (e.g. where a user has accessed a folder, or someone has attempted to login to your firewall). Providing analysis tools can enable staff to detect unusual behaviour (e.g. someone trying to access a folder they have no business need for) or investigate what happened after a cyber breach has been detected. Like other security tools, any monitoring capability will only be as effective as the information that it receives and stores, and therefore careful consideration should be given to which security logs are generated and ingested by the solution. Monitoring capabilities can range in cost and complexity from solutions that only use free opensource software for log analysis through to implementing a Security Operations Centre (SOC). For more information please see the link below: https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide

User Education and Awareness

Users have a critical role to play in their organisation’s security, so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as help to establish a security-conscious culture.

OVERALL RAG STATUS 🟩

Scoring:
15/15

Question Breakdown

🔴 **0** 🟡 **0** 🟢 **3**

Questionnaire Results: User Education and Awareness

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
6.1	Do you have an Acceptable Use Policy (AUP) for users? How often are users reminded of this?	Yes Every 12 months	Monitor the effectiveness of security training: Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training provided will allow for a two-way dialogue between the security team and users.	An Acceptable Use Policy (AUP) is a document stipulating constraints and practices that a user must agree to. Best practice is to implement an AUP and enforce the policy among any staff using company devices or personal devices inside of the organisation.
6.2	Do you provide regular refresher training on the security risks of the organisation to your employees? If so, how often?	Yes Every 12 months	Monitor the effectiveness of security training: Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training provided will allow for a two-way dialogue between the security team and users.	You should consider educating all staff on the current cyber threat on at least a quarterly basis if you are not already doing so. This can be done by using a Learning Management System (LMS) that covers all required topics.
6.3	Is there any disciplinary action taken if a user is found to not be complying with the organisations security policy?	Yes		Disciplinary action should be taken against non-compliant and repeat offenders. All sanctions should be clearly set out in the Acceptable Use Policy (AUP).

Incident Management

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

OVERALL RAG STATUS 🟩

Scoring: 20/20

Question Breakdown

🔴 **0** 🟡 **0** 🟢 **4**

Questionnaire Results: Incident Management

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
7.1	Do you have a specific incident management team, or named individuals responsible for Incident Management?	Yes		Your cyber incident management team may be a subset of a wider incident management team or a standalone team depending on your view of the likelihood of an attack. It may also include people from outside your organisation such as PR and media relations consultants and Cyber Incident Response teams to assist in responding to any incidents if you do not have the full range of skillsets in-house.
7.2	If yes, have the relevant individuals/team members had sufficient training (technical and non-technical) for their roles?	Yes		One of the key competencies for any Incident Response team is to be able to recognise and declare a cyber incident. Providing specialist training to certain team members can also have an added benefit of increasing cyber awareness across the organisation if those team members promulgate their knowledge and enthusiasm for the subject.
7.3	Have you ever tested your incident management capability? If yes, how recently was this?	Yes Last 12 months		There are various levels of testing that can be conducted, from senior executive level 'table top' exercises (to explore information flows), through to responding to cyber incidents and full technical simulation of an attack on a replicated network to allow your cyber team to see what a real attack looks like. These exercises are most effective when based on real examples and using up to date attacker Tactics, Techniques and Processes (TTPs). Conducting regular exercises can play a key role in educating team members and management. A lessons learned process is equally applicable to cyber exercises as it is to actual incidents.
7.4	Do you have a policy in place for management review of lessons learned after an incident?	Yes		All lessons learned should be reviewed by management and adjusted as seen fit. Appropriate steps should be taken to minimise the repetition of any incident, however large or small and the steps should be reviewed when necessary.

Malware Analysis

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

OVERALL RAG STATUS

Scoring:
10/10

Question Breakdown

0	0	2

Questionnaire Results: Malware Analysis

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
8.1	Do you conduct regular scanning for malware in your organisation?	Yes All of the above		Anti-virus tools are widely used across many organisations. However, if regular scans are not conducted then the chance of missing important security alerts such as the presence of malware are greatly increased. Conducting regular scans across your network will minimise the impact any malware/virus has had on your systems by limiting the time it has spent in your environment.
8.2	Does your web browser restrict access to certain sites? If so, how often are these rules updated?	Yes N/A		Access to certain sites should be restricted in a work environment. If it is against an organisation's policy to browse social media for example, then all access to social media platforms should be restricted. Some organisations will 'blacklist' sites that should not be used on work devices. This will block access for that specific URL/IP address but may be difficult to keep on top of due to the speed at which malicious websites appear online. Another option could be to create a 'whitelist'. This rule enables access to specified websites only. For example, your organisation could whitelist your company website as well as others that are vital for daily use. Any site or platform that was not on the whitelist would be implicitly denied.

Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

🟩 **OVERALL RAG STATUS**

Scoring:
25/25

Question Breakdown

🔴 **0** 🟡 **0** 🟢 **5**

Questionnaire Results: Monitoring

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
9.1	Do you currently collect, store and analyse logs from your systems and networks to identify threats?	Yes 3 months		Monitoring is an active concept that requires staff to be trained in how to respond to an alert from a monitoring tool and how to keep that tool up to date given the evolving cyber threat. Many organisations purchase monitoring software but then do not invest the time to keep that system up to date or have people monitoring any alerts generated by the system. Some alerting rules will always be valid (e.g. alert if someone gets their password wrong more than five times) and some will vary with evolving cyberattack methodologies (e.g. alert if Central Processing Unit (CPU) usage on the core router is above 90%). It can be complex to identify ‘unusual’ activity in systems, network traffic and user activities and there are a range of tools in the market that advertise their abilities in this area for large organisations. For smaller organisations it should be easier to manually analyse logs to look for indications of unusual traffic. Best practice is for organisations that outsource their IT to consider how their outsourcing partner implements monitoring of their network, and potentially request regular reports on this monitoring effectiveness as part of other IT Key Performance Indicators. As with all cyber security measures it is possible to implement monitoring solutions in a phased fashion to enable controlled financial outlay alongside incremental security improvements and staff training. This will enable the processes associated with running and maintaining

Questionnaire Results: Monitoring

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
				such a capability to be successfully absorbed for the long term.
9.2	Do you currently outsource the security monitoring of your networks or systems? If so, please describe level of monitoring?	No		Best practice is to ensure that you have an understanding of your own monitoring agreement, and what the agreement covers. This is extremely important if you choose to outsource security monitoring in the future. The agreement, at a minimum, should cover which log sources are being monitored, what attack types should be discovered and how often the detection rules are being updated. You should also consider asking any security provider to explicitly report on what threats their monitoring would not detect.
9.3	How confident are you in your existing security monitoring capabilities to detect unusual activity that could indicate an attack?	Very Confident		Many networks, no matter how strong, will have vulnerabilities. Best practice for securing any network is regular testing, whether through vulnerability scans or more in-depth penetration tests to identify any weakness and prevent a cyberattack.
9.4	How often are any automatic alerting rules updated in your security monitoring system? What triggers an update?	Yes Every month		Alerting rules should be updated regularly. These should take into account new threats such as new strains of malware, malicious IP addresses and Command and Control IPs. An out of date alerting tool is of much less value than an updated version.

Questionnaire Results: Monitoring

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
9.5	If you had to investigate a cyber incident would your system have sufficient logs to show who accessed what, when they did so and what they did to the information?	Yes	Align the incident management policies: Ensure that policies and processes are in place to appropriately manage and respond to incidents detected by monitoring solutions. Conduct a 'lessons learned' review: Ensure that processes are in place to test monitoring capabilities, learn from security incidents and improve the efficiency of the monitoring capability.	When designing a log collection system, best practice is that organisations should consider what logs they wish to store and for how long. Typically this is either articulated at a business level e.g. ‘we need to keep logs on user access for 3 months’ or based on available space e.g. ‘we can have a 100 GB log store and will configure it to overwrite the oldest data once full’. There are many vendors offering log management platforms who will also look to sell solutions around full network recording to keep all data flows as well as logs. If you invest in a log management tool, then it is important to consider how this is maintained and used so that it is effective if required for an investigation.

Removable Media Controls

Removable media provides a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls for its use.

OVERALL RAG STATUS

Scoring: 16/20

Question Breakdown

🟥	🟨	🟩
0	1	3

Questionnaire Results: Removable Media Controls

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
10.1	Can users use removable media (e.g. USBs)?	Yes – use a product that restricts what you can copy. Encrypted memory disk provided by IT team. Storing patient data requires specific written consent.	Produce corporate policies: Develop and implement policies and solutions to control the use of removable media. Do not use removable media as a default mechanism to store or transfer information. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms. Limit the use of removable media: Where the use of removable media is required to support the business need, it should be limited to the minimum media types and users needed. The secure baseline build should deny access to media ports by default, only allowing access to approved users. Formally issue media to users: All removable media should be formally issued to individual users who will be accountable for its use and safe keeping. Users should not use unofficial media, such as USB sticks given away at conferences. Encrypt information held on media: Sensitive information should be encrypted at rest on media. If encryption is not employed, then appropriate physical protection of the media is critical.	Blocking the use of removable media essentially removes one pathway that a potential attacker may use to infect your systems. However, if this is not practical for your organisation, an option is to limit removable media to either specific items or devices and ensure these are checked for viruses and malware in a secure environment (e.g. a standalone PC) prior to use on your main network.

Questionnaire Results: Removable Media Controls

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
10.2	Is removable media scanned for malware before being introduced to any system?	Yes		If your organisation requires the use of removable media, then best practice is that each device should be scanned prior to connecting to your network. This process is generally quick and easy to implement and drastically reduces the risks associated with USBs, removable hard drives etc. Again, a scanning tool is only as effective as its last update so ensure these are also updated regularly.
10.3	Is data encrypted before storage on removable media? If so, does it use default passwords or individual passwords?	Yes		There are a range of free media encryption tools that allow users to encrypt their removable media devices. Some users are worried about using encryption tools in case they forget another password, however, these can be configured to have public and private keys so that an administrator can always access data on the media if the user forgets their password. If used, then best practice is that organisations should ensure the passwords used with these media meet the same standards as network passwords to reduce vulnerability to brute force attacks.

Questionnaire Results: Removable Media Controls

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
10.4	Are you aware of your personal responsibility for following your removable data security policy if you have one?	Yes		Best practice is that all users are trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate it securely by following clear procedures. This would normally include direction on: • Secure storage and management of user credentials • Incident reporting • Environmental awareness (the risks from being overlooked, etc.) A more secure way to provide remote access to the organisation’s network is with a Virtual Private Network (VPN). A VPN creates a secure link between your network and your employee's computer across the Internet.

Home and Mobile Working

Mobile working and remote system access offer great benefits but expose new risks that need to be managed. You should establish risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

🟨 **OVERALL RAG STATUS**

Scoring:
5/10

Question Breakdown

🔴 1	🟡 0	🟢 1

Questionnaire Results: Home and Mobile Working

Ref	Question	Answer	UK NCSC Best Practice	Grant Thornton Comments
11.1	Do you have a published policy on mobile working? If yes, how often are staff trained on this?	No	Assess the risks and create a mobile working policy: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed. Educate users and maintain awareness: All users should be trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate it securely by following clear procedures.	A large number of organisations allow for mobile working. Best practice is that a separate policy should be generated and adhered to. This will cover potential risks associated with this type of use and specifically relate to issues only associated with mobile working e.g. connecting to public Wi-Fi.
11.2	Do your corporate devices use encryption at rest (e.g. laptops using encrypted disks and smart devices using secure software containers)?	Yes		Best practice is that encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted version of the same data.

Glossary

Term	Explanation
3rd party security breaches	Where an outside partner or provider with access to your systems and data suffers a security breach. In this case your data will be exposed to the breach too.
Cyber attack	An attempt by hackers, targeting a computer network or system, to expose, alter, disable, destroy, steal or gain unauthorised access, or make unauthorised use of an asset.
Encryption at rest	Data at rest means data that is not moving through networks – for instance the data on a laptop when it is not connected to any network or Wi-Fi etc. If this information is encrypted while at rest, then it means that if it is copied by a third party then that data will be protected by the encryption. Examples of encryption at rest include using full-disk encryption in Windows 10 or FileVault on Apple OS.
Multi factor authentication	A method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. For example, having a username, password and a onetime token/pin that is provided via software on a smartphone or via text message.
UK NCSC	United Kingdom National Cyber Security Centre
Phishing attacks	A cybercrime in which a target is contacted by someone posing as a legitimate institution, who lures individuals to provide sensitive data, such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access accounts and can result in identity theft and financial loss.
Software Framework	A foundation on which software developers can build programs and applications.
Spear phishing	Spear phishing is an email or electronic communications scam targeted towards a specific individual, organisation or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.
The Web	An information space holding publicly available data, accessible by the Internet.

Intentionally Blank

Grant Thornton

An instinct for growth™

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grantthornton.co.uk